Privacy Commissioner

Annual Report 1988-89

Annual Report
Privacy Commissioner
1988-89

89-05108/

The Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3
(613) 995-2410, 1-800-267-0441

© Minister of Supply and Services Canada 1989

Cat. No. IP 30-1/1989

ISBN 0-662-56842-7

"No personal information shall be collected . . . unless it relates directly to an operating program or activity . . . ".

"A government institution shall, wherever possible, collect personal information . . . directly from the individual to whom it relates . . .

". . . shall inform any individual . . . of the purpose for which the information is being collected.

". . . shall take all reasonable steps to ensure that personal information . . . is as accurate, up-to-date and complete as possible.

"Personal information . . . shall not, without the consent of the individual to whom it relates, be used . . . except

(a) for the purpose for which the information was obtained or compiled . . ."

(or in accordance with specific exceptions set out in section 8)

The *Privacy Act*

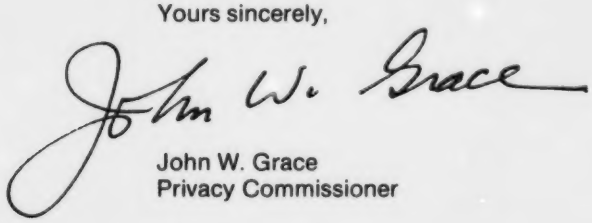
The Honourable Guy Charbonneau
The Speaker
The Senate
Ottawa

June 30, 1989

Dear Mr. Charbonneau:

I have the honour to submit to Parliament my annual report. This report covers the period from April 1, 1988, to March 31, 1989.

Yours sincerely,



John W. Grace
Privacy Commissioner

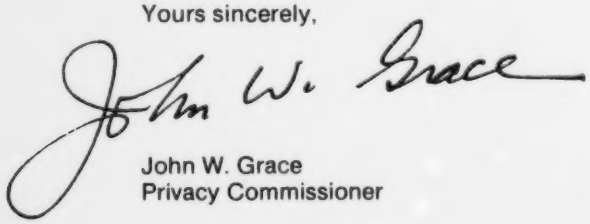
The Honourable John Fraser, P.C., Q.C., M.P.
The Speaker
The House of Commons
Ottawa

June 30, 1989

Dear Mr. Fraser,

I have the honour to submit to Parliament my annual report. This report covers the period from April 1, 1988 to March 31, 1989.

Yours sincerely,



John W. Grace
Privacy Commissioner

Contents

Mandate 01
A Mixed Review 02
Who's in Control Here? 10
AIDS and Privacy 14
The Dawn of the Biotechnological Age 16
Computer Security 18
CSIS Files 20
What's with the Cheque? 22
Complaints Directorate 24
  Cases 26
  Inquiries 38
Compliance Directorate 39
  Canada Post 42
  Pension Appeals Board 44
  Science Council of Canada 44
  Department of Finance 45
  Ministry of the Solicitor General 46
  Employment and Immigration Canada 47
Notifying the Commissioner 50
Spreading the Word 53
Corporate Management 54
Appendices
  I Organization Chart 56
  II Government Institutions covered by the Act 57

Mandate

The *Privacy Act* provides individuals with access to their personal information held by the federal government; it protects individuals' privacy by limiting those who may see the information; and it gives individuals some control over the government's collection and use of the information.

The Act sets out the principles of fair information practices, requiring government to:

- collect only the information needed to operate its programs;
- collect the information directly from the individual concerned, whenever possible; and
- tell the individual how it will be used;
- keep the information long enough to ensure an individual access; and
- "take all reasonable steps" to ensure its accuracy and completeness

Individuals in Canada may complain to the Privacy Commissioner if:

- they are denied any part of the information;
- they are denied their request to correct some of the information on the file — or their right to annotate it;
- the department takes longer than the initial 30 days or maximum 60 days to provide the information;
- the Personal Information Index description of the contents of the information bank is deficient in some way;
- the department's listing in the Index does not describe all the uses it makes of personal information;
- an institution is collecting, keeping, using or disposing of personal information in a way which contravenes the *Privacy Act.*

The Privacy Commissioner's investigators examine any file (including those in closed banks) except confidences of the Queen's Privy Council to ensure that government institutions are complying with the Act.

The Act also gives the Privacy Commissioner the power to audit the way government institutions are collecting, using and disposing of personal information.

A Mixed Review

The measure of a year's results in the privacy business can be as variable as the standards used for the calculation. It may even be fraudulent to attempt to sum up the privacy state of the nation with catchy generalizations. The subject is now simply too complex to be reduced to neat themes.

Even the Supreme Court of Canada mixed the results. Here was a year in which the court pronounced in *Her Majesty the Queen v. Brandon Roy Dyment* that "privacy is essential for the well-being of the individual" and the "restraints imposed on government to pry into the lives of the citizens go to the essence of a democratic state". The message could not be clearer or the source more definitive.

Here the court was re-inforcing its earlier opinion that the protection of "individuals from unjustified intrusions upon their privacy" is established by section 8 of the Charter of Rights and Freedoms ("everyone has the right to be secure against unreasonable search and seizure"). The judgment in the Dyment case, written by Mr. Justice G. V. La Forest, also set forth the following key principle: "If the privacy of the individual is to be protected, we cannot wait to vindicate it only after it has been violated....Invasions of privacy must be prevented and, where privacy is outweighed by other societal claims, there must be clear rules setting forth the condition in which it can be violated."

The *Privacy Act* is precisely a compendium of such rules. In two cases now, the Supreme Court has given the *Privacy Act* the strongest possible constitutional underpinning, making explicit the application of section 8 of the Charter to privacy protection.

Parliament can take some satisfaction in being ahead of both the Charter and the Supreme Court in having established by the *Privacy Act* the rules to control government uses of personal information collected from its citizens. Parliament is not always thus in advance of the courts in these litigious days.

But the privacy news from the legal front does not bring unalloyed joy. The Supreme Court of Canada's decision in *Stewart v. Her Majesty the Queen* appears to set back the cause. In this case, the court ruled that confidential information cannot be stolen because it cannot be considered property for the purpose of the Criminal Code.

In the case, a union, attempting to form a bargaining unit at a hotel, was unable to obtain the names and addresses of some 600 employees because management treated this information as confidential. A consultant hired by the union obtained the list through a security guard who, for a fee, copied the names from a list on the hotel's premises without removing, or in any way altering, the original document. The consultant was charged under the Criminal Code with counselling to commit fraud, theft and mischief to the private property of the hotel and its employees.

The Ontario Court of Appeal's conviction was overturned by the Supreme Court (in a unanimous decision). Mr. Justice Antonio Lamer wrote for the court that "confidential information is not of a nature such that it can be taken because if one appropriates confidential information without taking a physical object, for example by memorizing or copying information...the alleged owner is not deprived of the uses or possession thereof". The judgment went on to observe that "one cannot be deprived of confidentiality because one cannot own confidentiality".

With great respect, as lawyers ritualistically intone, these observations have alarming implications for the information society in general and the *Privacy Act* in particular. If the *Privacy Act* promises anything, it is the promise of protection for the confidentiality of personal information collected by government institutions. That fine legal point of whether one can own confidentiality is simply irrelevant to the important business of keeping sensitive information confidential.

If this non-lawyerly reading of the court's decision is correct, insufficient weight was given to the significant injury which can occur through unauthorized access to huge amounts of sensitive personal information held by both government and the private sector.

While possible commercial harm seemed uppermost, perhaps exclusively, in the mind of the court, terrible personal tragedy could be the result of the unauthorized disclosures of Royal Canadian Mounted Police investigation records, Canadian Security and Intelligence Service surveillance reports, Health and Welfare medical files — to stay with government.

Yet, the court seems to have said that records could be memorized — or copied (or photographed?) — without any criminal sanctions as long as documents are not physically appropriated.

Stewart v. Her Majesty the Queen did not receive the public attention it deserved. Had the information been sensitive health or financial records and not a mere list of names involved in a commonplace labor dispute, the outcry would have been enormous — and deservedly so.

The *Privacy Act* contains no sanctions. Until this Supreme Court decision, a theft conviction under section 298(1) of the *Criminal Code* or a fraud conviction under section 328(1) seemed detterent enough. Thus it has seemed unnecessary to argue for a sanction provision in the *Privacy Act*. Now the assumed Criminal Code support has been removed.

True, a breach of trust offence remains. It was the charge successfully prosecuted in the case of the Revenue Canada employee who stole the income tax records of some 16 million persons from a Toronto office of Revenue Canada. However, this offence would not be relevant in situations where confidential personal information is taken by a non-public servant or is elicited by deceit from a public official.

Shortly after the decision was delivered in *Stewart v. Her Majesty the Queen*, the Privacy Commissioner raised his concerns with the then Minister of Justice, the Honourable Ray Hnatyshyn. The Minister felt that, despite the Supreme Court's decision, the *Criminal Code* would continue to deter the improper disclosure of information by public officials. He reiterated the government's commitment to amend the *Privacy Act* to provide a statutory basis for the security standards now contained in the Security Policy of the Government of Canada. The Minister noted 1985 amendments to sections 301.2 and 387(1.1) of the *Criminal Code* which created offences dealing with the integrity of computer systems and services and which protect computerized data including personal information.

However, there continues to be a gap in the law which Parliament should close because significant amounts of personal information are held by government in paper files and since compromise of such information by outsiders cannot be ruled out.

The Supreme Court concluded in *Stewart v. Her Majesty the Queen* that Parliament and not the courts should decide what protection be given to confidential information. Parliament needs to act upon that invitation and protect the integrity of the *Privacy Act*.

In passing that Act, Parliament made an explicit commitment to Canadians that the confidentiality of their personal information held by government would be respected. That is the bedrock upon which this legislation rests. If confidential information can be appropriated with no fear of sanction because "one cannot own confidentiality" then the promise Parliament made in the *Privacy Act* has been, at the least, seriously eroded.

"Owning" confidentiality could be enormously more important than owning physical objects. They, after all, can be replaced. But the loss of privacy is non-renewable. Its loss is nothing less than losing control, a diminishing of human dignity.

Hold the Applause

If it was a good news, bad news privacy year from the Supreme Court, so it was from government. The fairest measure of the government's performance is to test it against its own key commitments and timetable set out in *The Steps Ahead*, which was issued in 1987 in response to the unanimous recommendations of the Justice and Solicitor General Committee. That entirely reassuring document was greeted in this report last year with something of the reverence that the Ten Commandments received at Mount Sinai. When put in place, it was said, the new policies and proposed amendments to the *Privacy Act* would make Canada's third-generation privacy legislation "as good as any in the world".

The government's "plan of action" called for achieving all its goals by the end of 1988. Specific commitments were made: "begin immediately" the process of bringing Crown corporations under the *Privacy Act*; establish the Personal Information Index (the guidebook to the government's holdings of personal information) as a data base and to make it available in machine-readable form. The processes may have begun, but more than a year later these commitments had not been realized.

Other target dates were not met. Directives covering consultation with the Privacy Commissioner on issues with data protection implications were to have been issued by spring, 1988. Amendments to the *Privacy Act*, including the promised statutory basis for information security standards, were to be introduced by the fall of 1988. A public education program on behalf of the *Privacy Act* was to be in place by winter, 1988. Not only were the dates missed, nothing had occurred in these matters as of March 31, 1989.

Of course, these were self-imposed deadlines. Under-estimating implementation difficulties because of over-enthusiasm should not be too much faulted. Besides, some key commitments were made good, if somewhat later than promised. The will to proceed with the unfinished business appears generally strong.

But the sluggishness and the slippages are disappointing.

The next 12 months will demonstrate whether *The Steps Ahead* will be meaningful or largely an empty metaphor. Will the walk in *The Steps Ahead* turn out to be a stroll in the park? In the privacy business today, the Queen's counsel in Lewis Carrol's *Through the Looking Glass* should be the guide:

> "Now, *here*, you see, it takes all the running you can do, to keep in the same place. If you want to get somewhere else, you must run at least twice as fast as that".

Two Steps Forward

In last year's annual report, the government was congratulated for making good on two commitments — a new policy controlling the government's own use of the Social Insurance Number (SIN) and new controls on the matching or linking of unrelated data bases. Alas, the government's pace did not match the Privacy Commissioner's enthusiasm. Though the SIN and data matching policies were announced earlier, final approval was given only in April, 1989 — technically outside this reporting year.

Yet, the cliché "better late than never" is appropriate in this case. A year's delay does not take away from the significance of the accomplishment. The data matching controls were described here extensively last year.

The tough new restrictions on the government's own uses of SIN are worth revisiting; they represent the most significant of the major commitments on which the government has made good. The President of the Treasury Board put the issue precisely:

"Many Canadians feel threatened by the use of the Social Insurance Number as a universal identifier. With the rapid development of computer technology, there is a growing concern that the SIN may be misused for linking personal information in ways that may pose a threat to individual privacy".

Thus was announced the "first step by the government" to cap its collection and use of the SIN. A large number of existing uses of the number are to be eliminated over five years and from now on any proposed new collection of the SIN for administrative purposes, other than an existing, approved list, is to be sanctioned by Parliament itself.

The new policy stands up against every natural bureaucratic urge in the public and private sector. It is the first time any government has attempted to roll back the use of its own numerical identifier. Omelettes are more easily and less expensively unscrambled (the estimated cost of $16 million may be low). But it's being done!

No more will the SIN be a public servant's principal employee number; the armed forces lose the SIN as the military service number. Applicants for permanent residence in Canada will not come with a SIN, nor will applicants for citizenship be required to submit to a SIN.

Commercial fishermen seeking permits, taxpayers applying for fuel tax rebates, candidates for grants and fellowships — all these and others are set free from the usages of the SIN.

It is something of a paradox that an age which has all but lost the concept of sin has so come under the sway of SIN. Babies have been given a SIN as a birth registration number in Prince Edward Island and some funeral directors are said to ask for the SIN of the deceased: thus SIN from cradle to grave; SIN even unto death.

In putting its own house in order, the federal government has new moral as well as legal authority to make good on yet another warning issued to other levels of government and the private sector. Continued mindless and insensitive demands for the SIN invite legislation — and that would be deserved.

...A Step Back

Just three months after the announcement of an enormously encouraging policy to control the SIN, Parliament passed amendments to the *Income Tax Act*, among which required Canadians to disclose their SINs to financial institutions where there had been no such compulsion before. Suddenly, even a bank account couldn't be opened without a SIN.

The new policy was designed to facilitate the reporting of interest income to Revenue Canada, an almost noble purpose. Unfortunately, little or no effort was made to notify the public in advance of the purpose of this new collection and use of SIN.

Despite government's promise to consult the Privacy Commissioner in initiatives affecting privacy, no consultation was undertaken before the legislation was introduced. The efficiency of tax collection was accepted by the government as justifying a new use of the SIN without any apparent consideration of the inherent privacy dangers.

In the complexity and detail of the amendments to the *Income Tax Act*, the extension of the SIN and its significance was missed by members of Parliament, the media and, yes, the Privacy Commissioner's Office. One simply did not expect such legislation to contain anything of interest to the business of privacy protection. Of course, the fact that it did demonstrates the vulnerability of privacy to assault from the most unexpected quarters.

The provisions in the new *Income Tax Act* amendments have, for the first time, made it a punishable offence to refuse to provide a SIN. Government institutions have had by statute and regulation the authority to demand SINs, mainly for such social programs as unemployment insurance and pensions. (No number, no coverage, no benefits). Now, no number and a $100 fine. (What happens for refusing to pay the fine is not clear. Two days in jail?)

Another precedent is established here. Until these income tax amendments, Canadians were required by law to give their SINs only to the federal government. Now they must confess their SINs to banks, trust companies, stockbrokers, credit unions, whenever and wherever they make what looks like an interest-bearing investment. Welcome to the computer society.

Of course, taxes should be paid. There is a relentless consistency in applying the new law once the $1,000 interest deduction was abolished. But the implications of the new demands for the SIN with the penalty for failure to comply are much more sweeping than anyone appears to have realized. The pity is that no one thought to ask or even to explain.

So soon after announcing the admirable policy to restrict the government's use of the SIN, thousands of private sector institutions (consider the number of bank branches alone!) are authorized to maintain new records systems with the SIN as the identifier. The fact that there is a fine of $5000 for misusing the SIN is small consolation.

...and Another

In *The Steps Ahead*, the government committed itself to extending the jurisdiction of the *Privacy Act* to cover Crown corporations and their subsidiaries. Such action would almost double the number of institutions covered and, most important, would give visible leadership to the private sector. In implementing the fair information practices, the government was putting its own full house in order.

Since many of these Crown corporations are in direct competition with private sector companies, the coverage by the *Privacy Act* conveys the strong message that the government believes data protection can be a complement, not an obstacle, to good business. Canada Post, after all, has been subject to the legislation for five years and in the face of significant competitive pressures finds that life under the *Privacy Act* does not hinder it commercially.

Though the bulk of the Crown corporations may yet be covered (members of the Privacy Commissioner's Office travelled as part of an awareness task force, meeting representatives of some 21 corporations), two significant omissions, as well as the general delay, have marred the government's initiative. Neither Air Canada nor Petro-Canada were included on the list of institutions to be brought under the *Privacy Act*.

Air Canada has been exempted because it no longer is a wholly-owned government creature — a dubious ground indeed because the government continues to maintain majority ownership, whatever the future may bring. That itself is reason to hold the government to its original pledge. It would be a dangerous precedent in this age of privatization if mixed ownership were enough to exempt Crown corporations from federal legislation. Until now, it has not. Air Canada itself remains subject to the *Official Languages Act* and, presumably, it would even if it were to be completely privatized. Surely the privacy rights of Air Canada's customers and employees are as important as their linguistic rights.

Other western democracies have recognized the need to bring under data protection codes the vast amount of personal information held in the computers of air carriers. If British Airways can live with the United Kingdom's data protection legislation, Air Canada should be able to live with the *Privacy Act*.

With Petro Canada, ownership is not the issue; Petro Canada is a Crown corporation, pure and simple. But corporation's management has resisted the *Privacy Act* because of perceived difficulties with its operations if it had to live within the Act's principles.

Perhaps Petro Canada's life would be made easier if, for example, the credit files of its customers or lessees did not have to be opened up to those customers or lessees, as they would have to under the *Privacy Act*. Being held exempt from the more onerous demands of human rights or employment equity laws would also make Petro Canada's life easier. But there is no chance of such exemptions. The argument for the legal protection of the privacy rights of Petro Canada's employees and customers is at least as strong.

If such high-profile institutions as Air Canada and Petro Canada were both to be excused from the *Privacy Act*, the government would be rightly viewed as undercutting its own commitments. Almost every institution, public or private, can conjure up reasons to be made exempt from oversight legislation — privacy or otherwise.

Via Rail could object to the *Privacy Act*, so could the Canadian Broadcasting Corporation. Yet both of these institutions (the CBC with some special provisions to protect its news gathering activities) are to be covered.

There may seem to be an air of blissful or naive unreality to a plea to bring two Crown corporations under the *Privacy Act* when the entire private sector, including federally-regulated companies, operates outside the Act. Why worry about Air Canada when other Canadian airlines fly the friendly skies unimpeded by the binding rules of fair information practices? Why insist that the customers of Petro Canada be given the benefits of the *Privacy Act* while those of all its competitors are left to fend for themselves?

Two more institutions in or out of the *Privacy Act* will not make much difference to the overall standard of privacy protection in the country. But if government doesn't insist that its own creatures obey the privacy rules of the road, the private sector is not going to be impressed by preachments to adopt codes such as the data protection principles of the Organization for Economic Co-operation and Development (OECD).

Self Regulation?

All of which raises the effectiveness of the government's effort to encourage private sector firms to respect those OECD guidelines to which Canada is signatory. The Minister of External Affairs' request to major companies to implement these guidelines in their organizations does not appear to have brought any discernible results.

The federal government met on two occasions with provincial governments to develop strategies to encourage the private sector to accept and enforce the guidelines. However, no agreement has apparently been reached as to what business sectors are to be targetted or the strategies to be devised.

The government needs a more vigorous approach. That is the least it can do in light of its rejection of the unanimous recommendation of the Standing Committee on Justice and the Solicitor General that the entire federally-regulated private sector be made subject to the *Privacy Act*.

That recommendation was not accepted (a decision which the Privacy Commissioner supported) because self-regulation seemed to be the preferred way to travel in a time when deregulation is in fashion. There have been faint stirrings towards self-regulation and there was no evidence of endemic or widespread abuses. Moreover, could a single privacy law be constructed to cover the diversity of the private sector — from banks to cable television companies? Perhaps not. There are practical limits to enforceable regulation in the age of microcomputers. A swollen Privacy Commissioner's Office with brigades of inspectors would give even privacy a bad name.

Self-regulation will be for most, including the Privacy Commissioner, the preferred option to government regulation. Recent "second generation" data protection laws (Ireland, Australia and Japan all adopted legislation within the past 12 months) have been much closer to Canada's model than to the "first generation" laws of Sweden and France which covered the private sector. Without more evidence of effective self regulation, however, the supporters of voluntary data protection codes will be increasingly hard put to defend their position.

Who's in Control Here?

The demands for personal data continue to grow exponentially and unchecked. Arthur Miller, who teaches law at Harvard University, says that his ability to fly depends not on the fact that he is standing at an airport counter waving a ticket. So far as the airline is concerned, unless the right numbers come up on a computer, "I do not exist. I am a mere three-dimensional version of the two-dimensional screen". Let Mr. Miller continue:

> "It's not just an airline reservations system. It has my name. It has my telephone number. It has my credit card number. It has who I'm flying with. Whether I've got hotel reservations or a car rental through the system...that's a dossier, and I know it."

And there are more dossiers. Arrive at a hotel and, he says, "you're not going to lay your head down on a Sheraton pillow unless its computer recognizes you. You put it all together and you realize that your life is controlled by one data bank after another, made possible by the computer."

It is a price for convenience and efficiency. No one is suggesting smashing the computers. But ground rules for the handling of the vast amount of personal information being collected should be put in place and respected. Data collections are available, on command, for making the important decisions about us. Arthur Miller is right:

> "We have come to understand that it is impossible to get insurance, to get credit, to get certain jobs, get certain government benefits without going through record clearance and record approbation — that people will be looking through our files. Who they are, we don't know. Where they are, we do not know. What the criteria for decision-making might be, we do not know."

We do know (or should!) that information about us in computers can be wrong. But without privacy legislation or working, effective voluntary codes, there is no opportunity to see and correct one's file. Without privacy legislation or enforced codes, there is nothing to stop the frightening growth industry in the sale and exchange of computerized personal information, of data chronicling personal consumption habits (traced through credit card transactions and direct mail orders) and charitable or political contributions.

Who's in control here? Is it individuals of their own information? Or is it personal information collectors and traders with their marvelous machines? To become a "data subject" should not mean becoming any less a human being. Should that ever be conceded, civilization has become subject to its machines and our information societies will have evolved, as Professor David Flaherty of the University of Western Ontario has warned, into "surveillance societies".

Professor Flaherty, an internationally-recognized authority on privacy and data-protection laws, put it in almost apocalyptic terms:

> "The various automated data bases now in existence make possible fairly integrated monitoring of individuals in Western countries. The proliferation of such information banks in both the public and private sectors, rather than the existence of any single one of them, poses the fundamental challenge to privacy interests. We need to think about the implications of such surveillance practices for the protection of human rights. In North America in particular, the application of information technology is galloping ahead of regulation and control".

Stripped of one's power to control what the world knows about oneself is demeaning and dehumanizing. There is nothing fringe or dilletantish about claiming privacy rights. They go to the heart of human integrity, of dignity and the kind of society we want. This is why privacy matters.

Privacy matters most of all between citizens and governments because the state has enormous power to extract and use personal information.

Yet, a privacy concordat covering the marketplace is becoming almost as important. Even when personal information is voluntarily given (in many transactions there is precious little voluntariness, e.g., an application for credit), well-defined rules have become essential if individuals are to have at least residual control over the uses of such information.

Some privacy experts, including Professor Flaherty, have come to believe that it is now too late for volunteer privacy concordats in the private sector. They argue that only legislation can control the powerful new technologies and give personal information at least a minimal level of protection. Back to battalions of privacy inspectors and very red bureaucratic tape!

Another privacy scholar, Professor James Rule of the State University of New York, advocated recently that the best way to protect informational privacy is by giving individuals a copyright interest in the commercial use of their own personal data. Information could not be sold or exchanged for value without an individual's permission. An ingenious, fascinating, even logical concept, though highly improbable and unenforceable.

These are desperate solutions, born of frightful visions. Surely there exists a middle way.

The voluntary rules of the privacy road such as the OECD guidelines are entirely sensible and, if implemented, offer some reasonable reassurances. But it has become time for government to treat volunteering in this business much as "volunteers" are traditionally found in the armed forces.

Federally-regulated firms, which the Parliamentary Committee recommended unanimously should be made subject to the *Privacy Act*, would be the place to start. In addition to pursuing more vigorously a cooperative strategy with the provinces to encourage voluntary compliance with the OECD privacy guidelines, the Government of Canada should take on the federally-regulated private sector in a second front of privacy protection activity. Develop effective privacy codes, within a specified time, they should be told, make them known to your customers and employees (who will be delighted!) or, yes, face legislation.

The proponents of privacy laws for the private sector are right about one thing — gentle exhortation has not much worked. But better first to turn the screw a little than impose the heavy apparatus of legislated privacy protection.

Dial Bell for Data

The Privacy Commissioner has not been merely watching these issues from the sidelines, content simply to grade the government's performance. He stepped into the fray upon learning, last November, that the Canadian Radio-Television and Telecommunications Commission was examining whether, to whom and under what conditions, Bell Canada could sell its telephone directory data base of white and yellow page subscriber listings in machine readable form. The initiative was not Bell Canada's but that of companies who have been eyeing Bell's data base with some envy.

This proposal offers chapter and verse on how real the pressure is for the massive exchanges of computerized personal information. At the same time, it is a textbook example of how a sensitive regulatory agency should be alertly aware of the stakes.

In a nice understatement, the CRTC noted that "the provision of this information in machine-readable form may heighten concerns related to customer privacy". "Heighten", indeed! Though nothing is more public than a telephone book, there are good reasons why phone customers should be worried. The Privacy Commissioner put them forward in a formal intervention which asked the CRTC not to require Bell Canada to offer its directories data base to anyone willing to buy.

The reason is this: a qualitative change takes place when names, addresses and phone numbers are moved from paper listings to electronic data processing disks. Special privacy dangers arise because of the infinitely greater accessibility, transmitability and transformability (even the words are ominous) of data in machine readable form. And nothing is closer to home than a telephone book.

One company has already transferred to a 4.7 laser disk the names, addresses and phone numbers of 7.9 million of Canada's 8.5 million households. It was a slow, expensive (more than $1 million, and this in Pakistan) job.

The phone book was only the start. The same laser disk includes the co-ordinates of each household to within one meter on a grid map of Canada, the names of neighbours, electoral districts, the length of time the occupant has been at that address. Information from 12 demographic fields (sold in aggregated form by Statistics Canada) offers census data as to probabilities of income, language, religion and children. All this is information in the public domain. But add credit card or banking information, if such information was to made available by fair means or foul, and the result is profiling of the population on a mass, systematic scale.

It is a marketer's dream — a privacy nightmare. Machine-readable listings mean that personal information can be manipulated in any number of creative ways for telephone or mail soliciting. Yet, that would be an almost benign use. Such listings also provide a monitoring or tracking tool of interest not only to marketers but to criminals and, yes, law enforcement agencies alike.

Phone subscribers never dreamed of, much less consented to, this degree of privacy invasion just by the fact of being listed in the telephone directory. Technology makes the danger real and present.

AIDS and Privacy

On another front, and as promised in last year's annual report, the Privacy Commissioner developed recommendations to ensure that AIDS-related personal information is handled by the federal government in accordance with the letter and spirit of the *Privacy Act*. The resulting report, entitled *AIDS and the Privacy Act*, confirms that an appropriate national response to AIDS is perhaps the most sensitive and anguished privacy issue of our time. *AIDS and the Privacy Act* seeks an elusive balance between protecting the privacy of those either with AIDS or infected with the HIV (the virus that causes AIDS), and appropriate disclosures which the protection of others demands.

Compassion towards those afflicted demands that they are protected from the further trauma of unnecessarily invading their private lives and disclosing their condition. The diagnosis of AIDS continues to be a sentence to death. In fact, some current opinion suggests that simply carrying the HIV virus also means early death.

Unthinking and extreme public or government responses to the disclosure of AIDS or HIV infection may, and in some cases have, altered the very conditions of an individual's membership in society: access to schools, work, medical care, even family and friends. That is the simple case to be made for the deepest possible respect for the privacy of the victims.

On the other side, however, disclosure is required, though not nearly as often as is sometimes suggested. Scientific and medical communities may need to know who are the AIDS victims and HIV carriers in the quest to slow, stop or treat the disease. These competing concerns often call for conflicting courses of action.

The report concludes that mandatory HIV antibody testing of such groups as public servants, inmates of federal prisons, immigrants and long-term visitors to Canada, would contravene the *Privacy Act*. The *Privacy Act* prohibits the collection of personal information which is not related directly to a program or activity falling within the statutory mandate of a government institution. Such testing is not a necessary element of any present legislated program.

Of course, Parliament has the authority to override the *Privacy Act* and give government the power to subject groups of individuals to mandatory HIV antibody testing. However, any such action would represent an hysterical over-reaction to the AIDS epidemic — at least so it appears in the present state of knowledge about the disease.

Any public health benefits that would be achieved through large-scale testing are dubious at best and would be far outweighed by the devastating invasion of privacy which would result. Fortunately, privacy interests accord with the most informed medical opinion that AIDS testing should always be voluntary with pre-and post-test counselling.

The Government of Canada has an important leadership role to play in ensuring that AIDS is sensitively handled in the workplace. The report urges Treasury Board, as Canada's largest employer, to issue a comprehensive policy on AIDS in the workplace.

Confidentiality is an integral part of the workplace policy suggested by the World Health Organization. The employee should not be obliged to inform the employer about his or her HIV status, nor is there any need to inform co-workers. If AIDS-related personal information is volunteered, it should be accorded a high degree of protection and, prior to employment, there should be no direct HIV screening (testing) or indirect screening (assessment of risk behaviors or questions about previous tests).

One of the reasons most often given for individuals hesitating to undergo voluntary HIV antibody testing is the fear that they will not be able to control the extent to which third parties will be given access to the information. Indeed, the *Privacy Act* itself sets out some 13 circumstances in which government departments may disclose personal information to third parties without consent. In recognition of the particularly sensitive nature of AIDS information, *AIDS and the Privacy Act* recommends that a tightly controlled process be followed before any such disclosures are made.

Most important, the decision of whether to disclose to third parties without consent should be made only by the head of the government institution. The decision should be based on a consideration of:

1. why disclosure is necessary,
2. the potential adverse consequences of the disclosure on the individual(s) to whom it relates,
3. the likelihood that the requestor can and will maintain the confidentiality of the information, and
4. the likelihood that the requestor will use it only for the purpose for which it was originally sought.

The onus should always be on the requestor to justify the need to release the information without the consent of the individual(s) to whom it relates.

These recommendations attempt to reflect an appropriate compromise between privacy concerns and the legitimate needs of some government institutions. Changes in the understanding of AIDS, its transmission, in public attitudes may compel re-examination of the recommendations as, of course, would a vaccine or cure. In the words of the report:

"To hope for an early cure or an effective vaccine is a natural human response to this terrible disease. But hoping does not diminish society's responsibilities today. The principles set forth here in responding to the privacy issues in handling the personal information of those affected by HIV infection and AIDS may not give much long term comfort. But at least they make society's response more humane. For the moment, perhaps, that is the best we can do."

The Dawn of the Biotechnological Age

By-and-large, the government collects information about individuals in traditional ways, such as by surveys, forms, letters or direct observation. But even these old-fashioned methods can be abused, resulting in unacceptable invasions of privacy. More ominously, however, intrusive collection techniques are gaining currency.

Such methods (some newer than others) permit information about individuals to be drawn directly from their biochemistry: i.e., the breathalyzer and polygraph. Urine tests, blood tests and genetic mapping are also becoming fashionable as means of finding out a person's hidden (perhaps even from himself or herself) secrets.

While these information collection techniques are best known in the law enforcement environment, they are achieving increasing popularity for screening purposes outside of the criminal justice sphere. Would you be a loyal and trustworthy employee? Would you engage in behaviour likely to put others at risk? Have you broken the rules governing an activity in which you want to engage? Do you have a genetic predisposition to certain diseases or personality styles? Governments and private sector employers are being tempted to seek access to biochemistry to provide answers to these questions.

The Department of National Defence, for example, tests the blood of its employees wishing to attend U.S. defence courses to determine if they are HIV free. The Canadian Security Intelligence Service gives prospective employees a polygraph test to determine whether they are loyal and trustworthy. Transport Canada is considering whether transportation workers should have their urine tested for the presence of illegal drugs.

Sports Canada is urging that the urine of funded athletes be tested for the presence of banned (not necessarily illegal) drugs which could enhance performance and undermine fair sporting competition. The RCMP is using genetic material for identification and a national "genetic fingerprint" inventory will be developed similar to that which now exists for fingerprints. Moreover, research is underway into techniques which would enable detailed physical and behavioural profiles to be developed on individuals based on a DNA test.

One commentator has argued that we are moving from the information age into the biotechnological age. In that transition are privacy dangers the likes of which we have not seen in our history.

If privacy is to have any meaning in the 90s and beyond, great care must be taken to ensure that effective limits are placed on new, more intrusive means of information collection. Yet as we end the 80s there are indicators that the policy-makers may not be so inclined.

Some officials testifying at the Dubin Inquiry strongly advocated mandatory, random and unannounced urine testing of federally-funded athletes. While a strong case can be made for such testing, it is troubling that a government policy, even in a well-defined area and with tacit consent of the athletes, appears to ignore a concept which is fundamental to individual privacy — the presumption of innocence. The need to prevent intrusions into private lives, unless there is a specific and reasonable suspicion of wrongdoing, has been clearly articulated by the Supreme Court as part of Canada's Charter of Rights and Freedoms. It has only been compromised in rare instances to protect life — instances such as random, roadside alcohol tests.

Yet, in the case of athletes, the country's offended national pride seems to be widely accepted as sufficient reason to ignore a fundamental principle of freedom. If we can justify the intrusions necessary to test athletes, and perhaps Mr. Justice Dubin will conclude that we can, will it not become easier for employers to justify intrusions into the bodies of their employees or potential employees? Canada's inquiry into drug use by athletes may have an impact on our philosophy of individual privacy which will not end in the sports arena or at the locker room door.

The principle reason why these annual reports have expressed concern about computer matching — the comparison of unrelated data bases to compile profiles of certain individuals — is because it represents search and seizure of records without reasonable cause. For the same reason, the Privacy Commissioner will continue to monitor developments in biotechnological screening programs in an effort to protect the privacy of innocent individuals.

Computer Security

> "...security is concerned with protecting the computer from people; privacy with protecting people from computer"
>
> (Robert P. Bigelow)
> Computer Law and Security Report, March/April 1989

Would it were as simple! In highly automated office environments, good computer security is essential to protecting people from other people — perhaps the ultimate goal of privacy advocates.

A totally secure computer system would appear to be an unattainable ideal in the current decentralized data processing world. Computer security professionals now talk of "trusted" rather than "secure" computer systems. (It's a telling social comment that the term "trust" now implies a measure of distrust!)

We are now in the young adulthood of the age of management information systems (MIS). Since the mid-70s the ability of the computer to perform multi-processing, to manipulate massive files, to pass information over great distances in seconds and to allow many users to share the information resource has proven an integral part of the administration of government.

It is no longer uncommon to enter a government office and find multi-purpose workstations connected to a mainframe computer system or to a network of computers wherein the data and, in some cases, the logic programs are purposefully or unwittingly shared.

Over the past year the Office of the Privacy Commissioner delved into the labyrinth of computer security — a confusing world of specialized terminology and technology. Internal threats to computer systems come in strange forms: salamis, trap doors, logic bombs, Trojan Horses, and worms. External threats are equally exotic: viruses, spoofing, scanning, switcheroo, network weaving and pass through.

And those who seek to counter these threats also "colour" the issue; in the U.S. the Department of Defence security standards are published in the "Orange Book" and explained in the "Yellow Book". The security of networking systems are dealt with in the "Raspberry Book" — and so it goes.

The security challenges which the MIS environment poses are enormous and the Office of the Privacy Commissioner is in its infancy in developing the expertise to pinpoint problems and offer responsible, workable solutions. In the coming year, special emphasis will be placed on the security of EDP systems during our regular privacy audits of government institutions.

Special tribute should be paid to the work of the System Security Centre of the Communications Security Establishment. The Centre was established in August of 1988 to augment the computer security expertise of the RCMP and DND and to provide new capabilities for the evaluation of computer and network security products for the Government of Canada. Part of the impetus driving Canada to develop its own trusted computer security evaluation criteria was the *Privacy Act*. There was a recognition that, although the protection of national security information poses the most difficult technical problems, the most widespread problem was the need to protect the privacy of personal information held by government.

The Privacy Commissioner welcomes this initiative and looks forward to a continuing exchange of information and ideas with the Systems Security Centre.

CSIS Files

Another collection of highly-sensitive personal information continued to be a matter of concern over the past year — the intelligence files inherited by the Canadian Security Intelligence Service (CSIS) from the former Security Service of the RCMP. Much of the information contained in these files does not, at least in the view of the Security Intelligence Review Committee, meet the tests for collection under the *CSIS Act* now that the definition of "threats to the security of Canada" has been more precisely drawn.

Thus, CSIS finds itself in the awkward position of being the custodian of information about individuals which it would not be entitled to collect under the terms of its present mandate.

The solution seems simple — dispose of the old files!

In fact, CSIS has set up a unit to review the files, extract what is of continuing legitimate significance to CSIS and dispose of the rest. But, the process is laboriously slow; — some of these files have been "sequestered", others have become subject to special rules governing internal access to and use of the files. Consultations are in progress between CSIS and the National Archives to determine what information should be archived and under what conditions.

Yet, the shredders do get used! Since the lifting of the file destruction moratorium imposed in 1985 (after concerns were expressed by the Deschênes Commission on war criminals), some 120,000 security service files have been disposed of. This includes 67,000 which had previously been scheduled for destruction by the RCMP, and 53,000 reviewed prior to disposal by CSIS. It is comforting that the review has resulted in CSIS keeping fewer than 100 files. There remain, however, many thousands of files whose appointment with the shredder is years away.

These old RCMP files create a further complication for CSIS. As authorized under the *Privacy Act*, CSIS will neither confirm nor deny the existence of information which is of continuing intelligence value. Such information is contained in bank SIS/P-PU-010. Neither will it confirm nor deny the fact that no information exists when a *Privacy Act* request is made to that bank. Both the Privacy Commissioner and the Federal Court of Canada have accepted that the so-called "mosaic effect" requires CSIS to take this approach.

However, CSIS will confirm the existence of certain personal information which was gathered by the former RCMP Security Service. Dated, less sensitive information of this type is maintained in bank SIS/P-PU-015. Its existence will be confirmed and the information will be released to a requestor subject to any of the specific exemptions which are set out in the *Privacy Act*. It has not proved possible to reach agreement with CSIS on a set of guidelines which would define what constitutes "less sensitive" information, this despite a genuinely good faith effort on the part of CSIS to respond to the concerns raised by the Privacy Commissioner in his last annual report.

As requests are received, CSIS decides where to allocate (bank 010 or 015) the former RCMP Security Service intelligence information. This appears to be the only practical approach until all records are disposed of which do not meet the *CSIS Act's* collection requirements.

The Privacy Commissioner is pleased to report that CSIS plans to accelerate its review and disposal of files. In the next two years it intends to review for disposal twice as many as during the past five years. The Privacy Commissioner applauds the initiative but considers the process should be independently monitored to ensure that all information which does not meet the "strictly necessary" requirement of section 12 of the *CSIS Act*, is actually disposed of and not merely recycled into other formats.

The Inspector General (under sections 30 and 31 of the *CSIS Act),* the Security Intelligence Review Committee (under section 40 of the *CSIS Act)* and the Privacy Commissioner (under section 37 of the *Privacy Act*) all appear to have the power and mandate to provide such independent inspection.

The Privacy Commissioner will, in the coming months, consult with the relevant parties to determine how this file disposal monitoring can be carried out without unnecessary duplication of effort.

What's with the Cheque?

Mailing lists are a private sector privacy issue which everyone understands. But few in the private or public sector have mailing lists as up-to-date and complete as the federal government.

Consider just three.

- the government's own employees (including the armed forces and the RCMP) 350,000;
- family allowance/old age pension/ Canada Pension Plan recipients' list, (approximately 5.5 million names and addresses);
- and the income tax list (about 17 million).

These three lists would be a veritable gold mine for direct mailing. Some brazen requests for them have already been made.

Item: A publishing house asked Health and Welfare for the list of all Canada Pension Plan recipients and applicants. The reason? To send an advertising brochure offering legal services to anyone with a pension problem.

The federal government is prohibited from selling (or giving away) its mailing lists. But what about the government's own use of its lists. Government departments and agencies have recognized government cheque envelopes as a cost-efficient method of communicating with their clients. The cost of enclosures with regular government mailings pales beneath that of an advertising campaign and targets more successfully. It would even be an excellent way of advertising the blessings of the *Privacy Act*! ("Do you know your privacy rights?")

Family allowances and pension recipients are accustomed to finding information notices with their monthly cheques. Privacy violations or not?

No violation providing the information relates directly to the mandate of the department on whose behalf the cheque is issued. Thus, Health and Welfare Canada can appropriately inform pensioners of changes in benefits or remind parents to keep their children's innoculations up-to-date.

But there is potential for abuse. To its credit, this has not escaped the attention of the Treasury Board. As a result, the board now requires departments to obtain its permission to enclose material with a regular government mailing. The record is generally good. However, in spite of the closer monitoring, some five of the 50 mailings last year were unrelated to the original purpose of the mailing list.

Examples: Information on the Canada-U.S. Free Trade Agreement was offered in one enclosure which was sent to all nine million recipients of Family allowance, Old Age Security and Canada Pension Plan. Pension and salary cheques to past and present public servants were accompanied by appeals to purchase Canada Savings Bonds and to contribute to United Way campaigns.

Clearly, there are conflicting goods here. The government's own communication policy sensibly obliges departments and agencies to tell the public about their activities. Canada Savings Bonds are essential to the government's financing and individuals wanting to buy undoubtedly value knowing about the bonds and the procedures for automatic deductions. As well, the United Way depends heavily upon public servant's contributions, which are greatly facilitated by payroll deductions.

Yet, the principle in the *Privacy Act* is clear. Information collected for one purpose cannot be used for another purpose.

There will be some difficult applications of the law, some hard judgment calls. The Privacy Commissioner seeks not to be the Grinch who stole the Christmases which United Way agencies provide. But the Privacy Commissioner very much wants to stop government mailings being used for distributing political statements. Government junk mail is still junk mail.

What accompanies a government cheque bears some close watching.

Consultations are underway with Treasury Board to set guidelines to ensure government mass mailings conform with the *Privacy Act*.

Complaints Directorate

This year's startling 20 per cent increase in new complaints (1,050 compared to 691 in 1987/88) is difficult to explain. It may simply reflect a return to the pattern of a 10 per cent annual increase evident since the program began, making last year's drop an aberration for which this year's caseload compensated with a vengeance. This can be said: there is no reason to attribute the increase to growing resistance to either the letter or spirit of the *Privacy Act*.

The return to the larger numbers was accompanied by more complaints about the length of time departments took to respond to requests. This is disappointing. The Commissioner had hoped that the delay problem would resolve itself as departments gained experience. In fact, the office investigated 414 delay complaints, 243 of which were against the Correctional Service of Canada (CSC) — the result of a marked increase in applications.

Despite the substantial rise in new complaints, the Commissioner and his staff whittled away the 296 cases carried over from last year. Only four of these now remain.

Overall, investigators completed 1,028 cases during the year, an increase of 56 per cent over the preceding year. The directorate continues to reduce the time required to complete an investigation. The new performance standard for an investigation is three months (on average), with no complaints outstanding for longer than six months. At the end of the reporting year, 94 per cent of the complaints were less than six months old.

The acceleration can be partially explained by the addition of three staff positions to the directorate, given in anticipation of Crown corporations being made subject to the *Privacy Act*. By the end of the year these corporations were still not covered so the additional investigators allowed the office to keep pace with the large increase in complaints. With the directorate now fully staffed, the office is confident of continuing to meet the new performance standard — at least until the Crown corporations come on stream.

Statistics — "a rose by any other name"

The terminology in this report describing the disposition of complaints is a little different from previous years. The change makes consistent the terminology used by the departments in reporting their statistics to the Treasury Board and that of the Privacy Commissioner's office. Discussions with the board and all other parties resulted in the following:

Not well-founded
(formerly "dismissed")

Well-founded, resolved (formerly "justified"). This means that negotiations led to what the Commissioner considered a reasonable resolution of the problem. It does not always mean that the complainant was completely satisfied.

Well-founded. This signifies that there was some breach of the *Privacy Act* which was not resolved, either because material could not be found, had already been destroyed, or time limits had been exceeded. This term is also used when access has been denied and the Commissioner has threatened to take court action in order to have the information released.

Abandoned. This indicates that the complainant has withdrawn the complaint (often because the problem has been solved before the investigation begins), or has not responded to follow-up calls or letters.

Origin of Completed Complaints by Province and Territory

Newfoundland	3
Prince Edward Island	35
Nova Scotia	17
New Brunswick	165
Quebec	240
National Capital Region Quebec	4
National Capital Region Ontario	53
Ontario	200
Manitoba	21
Saskatchewan	96
Alberta	57
British Columbia	134
Northwest Territories	1
Yukon	0
Outside Canada	2
TOTAL	**1028**

Cases

CEIC can seek UI medical claim details

An Ontario man objected to the amount of medical information the Canada Employment and Immigration Commission (CEIC) collected when he claimed unemployment insurance medical benefits.

The man was on modified duties at the time of his layoff because of an injury. He gave CEIC information from his doctor that stated the recuperation period and his claim was accepted. A week later, a specialist extended the recuperation period because the injury was not healing well. Later, the period was extended again. Each time he informed CEIC.

Following the second extension, CEIC asked for and received a completed form from the doctor. However, the commission found the information to be insufficient and asked for more detail. The doctor completed the form reluctantly because he considered the details privileged information.

During investigation it became apparent that the two doctors had supplied conflicting information. When this happens, CEIC requires, and is authorized to get, a diagnosis to settle the claim. The Commissioner concluded that CEIC officials were exercising prudent judgment as set out by the Unemployment Insurance regulations, by corroborating the information. He considered the complaint not well-founded.

Marriage data needed for passport

An Ottawa man complained that he had had to reveal his past and current marital status to the individual who guaranteed his passport application. He also worried that External Affairs collected too much information in his application.

Passport applications ask "if you are or have been married". The form explains that the details are needed for "identity, citizenship and/or custody of children." However, investigation revealed that the information is required in only three instances when:

*the surname on the passport was assumed after marriage (either the spouse's surname or a combination of birth surname and spouse's surname);

*when children are to be included on the passport (the details help determine legal custody);

*a female applicant was married to a non-British subject prior to January 1, 1947. She may have ceased to be a British subject because of the marriage and, according to the laws at that time, not a Canadian citizen.

In all other cases, passport examiners may waive the marriage data requirement.

The Commissioner agreed that External Affairs needed the information but questioned whether the application form made it clear that it was limited to the three circumstances. External Affairs agreed to explain this on a new form.

The Commissioner rejected the position that requiring the guarantor to know marriage details was an invasion of privacy. A guarantor is not simply a witness to the applicant's signature, but attests, to the best of his or her knowledge, that the information is correct.

"Since a Canadian passport allows the bearer to enter Canada ...as a matter of right, I believe that disclosure of the information to the person attesting... cannot be viewed as an unreasonable requirement", the Commissioner said.

He considered the complaint not well-founded.

RCMP may release subpoenaed information

A lawyer involved in a lawsuit with an insurance company complained that the RCMP had, without consent, given the company's lawyer a copy of his client's statement to police.

The RCMP explained that it had discussed that portion of the file with the company's lawyer but had neither provided a copy nor allowed her to see one. However, all the information had been subpoenaed at an earlier criminal trial of another man. The RCMP produced the information in response to the subpoena and it was now part of court records. Thus, the RCMP discussed nothing which had not already been disclosed at the trial.

The complaint was dismissed because the *Privacy Act* allows government institutions to release personal information in response to a subpoena.

No charge to use *Privacy Act*

A senior citizen complained when charged $25 to use the *Privacy Act*. He had seen information about using the Act in the *Seniors Guide to Federal Programs and Services*, a Health and Welfare Canada publication. He applied to National Archives for his employment file and to Canada Employment and Immigration Commission (CEIC) for his immigration file.

National Archives redirected his application to his former employer and shortly thereafter he received the information. However, CEIC charged him $25 for his immigration documents. Because the guide had not mentioned a charge, he wrote to Health and Welfare suggesting it include such information.

An investigator found that CEIC staff had misunderstood the man's request. Seniors often need certified copies of landing documents to support pension applications, a service for which CEIC charges. Once CEIC realized the request was not for certified copies but simply to see the file under the *Privacy Act*, it refunded the $25.

The complaint was well-founded/ resolved.

Keep performance appraisals five years

A complaint that a department was keeping employees' performance appraisals too long ended up involving Revenue Canada/Customs and Excise, National Archives, the Treasury Board and the Privacy Commissioner.

The complainant told the Commissioner that Customs and Excise was retaining annual appraisals longer than the three years described in the *Personal Information Index*. The length of time that appraisals are held (the retention schedule) is established by National Archives in consultation with the Treasury Board. Customs and Excise considered the schedules as policy, not law, and not subject to complaint. Treasury Board, however, considers the schedules to be the law.

The Commissioner agreed to study the matter. The investigator confirmed that Customs and Excise was keeping the man's appraisal (and all appraisals) beyond three years. Through consultations involving the department, Treasury Board and National Archives, he discovered that Treasury Board had changed the retention period to five years but the department had not been made aware.

After discussion, Customs and Excise concluded that the intent of Treasury Board's policy was clear and agreed to comply with the five year period.

Test scores need expert interpretation

A lawyer preparing an appeal sought information about her client from two Correctional Service of Canada (CSC) banks. She complained when CSC withheld information.

Investigation revealed that much material in the Offender Health Care Record bank was supplied in confidence by a province, and thus CSC was obligated not to release it under the *Privacy Act*. The investigator suggested that the lawyer apply using the provincial privacy legislation.

CSC had also exempted raw psychological test data from a Psychology bank, maintaining that releasing medical information would not be in the inmate's best interests. CSC argued that releasing test results in raw form would make it subject to misinterpretation by laymen.

According to a CSC psychologist, the test is copyright and psychologists are not free to provide copies. He also argued that revealing test questions, individual responses and scores would render the test invalid — particularly in a closed population like a prison. Further, test results can vary daily according to the subject's health or mood. Again, a layman might misinterpret such variations and one-time scores.

The doctor suggested that the lawyer hire a registered psychologist as an expert witness to whom the doctor could release the documents.

The Commissioner found compelling the doctor's arguments against releasing this type of information in a prison environment and considered the complaint not well-founded.

Applicant gets reference comments only

Several potential and former RCMP members applied for information from their security clearance records and complained when the Force withheld the names of persons interviewed during the security clearance process and their comments.

The RCMP argued that it must take extraordinary care in screening police officers. For example, police officers have the power to arrest and carry firearms. Temperament and moral character are therefore of special importance. The RCMP argued that it must protect its sources to ensure candor.

After discussing the complaints with the investigator, the RCMP staff agreed to review the material. It concluded that the sources' comments could be released, but it withheld their names (or other identifying details) to protect the integrity of the inquiry.

The Commissioner agreed with the resolution and considered the complaints well-founded but resolved.

World War II hospital records gone

Despite a thorough effort by National Archives, a British Columbia man did not receive all the information he wanted from the Archives' Medical Records World War II bank.

He told the Commissioner that the material Archives sent excluded documents from his stay in a particular hospital in the 1940s. This included a form he had been required to sign stating that he would not apply for a military pension.

At the request of an investigator, Archives searched other banks but with no success. Archives found the records of the hospital (which no longer exists), but lacked those of the period covering the complainant's treatment.

The investigators then asked the Department of Veterans Affairs who also searched, without success, for the missing files.

The Commissioner concluded that the files cannot be found and that Archives had responded to the best of its ability. The complaint was not well-founded.

Informant's name withheld in tax case

A woman complained to the Manitoba Institute of Chartered Accountants that her former chartered accountant had acted unprofessionally. The institute began an investigation and applied to Revenue Canada, Taxation on the woman's behalf for her individual income tax return file.

Revenue Canada withheld some information because it either concerned another person or its release could "be injurious to the enforcement of the *Income Tax Act*".

The lawyer complained to the Commissioner.

The investigation confirmed that some of the information was about someone else and was thus properly exempt. The rest concerned a confidential source. The Commissioner agreed that release of the material could threaten enforcement of the *Income Tax Act*. However, he added that a strong argument could be made that the public good would be best served by releasing the information. Nevertheless, the *Privacy Act* gives the department discretion to decide and he did not believe that Revenue Canada had exercised the discretion improperly.

The complaint was not well-founded.

Grounds of Complaints and Investigation Results

Grounds	Aband.	Well-founded	Well-found. Res.	Not Well-founded	Total
Access	16	8	69	410	503
Use & Disclosure	6	8	7	29	50
Correction/Notation	0	1	6	10	17
Time Limits	4	317	14	79	414
Language	0	1	0	23	24
Index	0	0	0	0	0
Collection	2	1	2	12	17
Retention/Disposal	0	0	0	3	3
TOTAL	**28**	**336**	**98**	**566**	**1028**

Employer compares sick leave records

A woman asked the Commissioner's Office whether Canada Post, which employed both her and her husband, could use her attendance records to investigate her husband's attendance problems. Her file had been given to a supervisor to whom she does not report and her husband found one of her attendance cards in his own file.

The investigation had to determine whether it was proper to match the couple's attendance records to verify her husband's attendance.

Canada Post considered the use consistent with the purpose for its collection—to ensure that employees respect their leave entitlements in the collective agreement. Canada Post held that when management suspects abuse, it was "natural" to review attendance records "including those of two or more individuals where warranted".

The Commissioner advised Canada Post that, while he understood the motivation, the practice appeared to contravene the *Privacy Act*. He invited Canada Post to respond before he made a final decision.

Canada Post replied that matching "supported the attendance and leave function" when management suspects employees are colluding to abuse leave. Canada Post maintained that the only option to matching records to confirm fraudulent leave claims would be an even more intrusive investigation.

The Commissioner was unconvinced. He had difficulty accepting that unregulated comparisons between the attendance records of spouses, other family members and golfing buddies were integral to attendance management. He concluded that accepting the position was tantamount to discrimination against employees whose relatives or friends also worked for the post office. He recommended that Canada Post stop the comparisons.

Canada Post did not agree but was prepared to discuss a resolution. After further negotiations, Canada Post adopted guidelines to control the practice. Under the new guidelines, individuals' attendance records will continue to be reviewed but will only be matched with those of others to generate depersonalized information or, if necessary, to confirm or disprove a pattern of common absenteeism already observed among employees.

The guidelines also restrict who may see and compare the information and to whom it may be disclosed.

Can't use tax files for discipline

A tax auditor, fired for falsifying her income tax returns, complained to the Privacy Commissioner that Revenue Canada, Taxation had breached both the *Income Tax Act* and the *Privacy Act* when it used her tax returns for disciplinary purposes.

A week prior to filing the complaint, the woman had asked the Federal Court to declare that Revenue Canada could not use the tax return information, except as allowed by the *Income Tax Act*. In particular, she argued that her tax returns should not be used as evidence in a hearing about her discharge.

The Commissioner postponed his finding until the court ruled. The judge agreed that when Revenue Canada is acting as an employer, it is not entitled to use individual tax returns for personnel purposes.

The *Privacy Act* allows the department to use personal information only for the purpose for which it was collected, "subject to any other act of Parliament". Since the use was not one for which it was gathered, nor was it a correct use under the *Income Tax Act* according to the court, the Commissioner concluded that the complaint was well-founded.

This does not mean that Revenue Canada may not discipline employees who evade taxes. It does mean that the department should treat the employee as it would anyone else it suspects of tax evasion, then take appropriate disciplinary action if he or she is found guilty.

Ham radio operators' data released

An amateur radio operator complained because the Department of Communications (DOC) releases amateur broadcasters personal information to amateur radio societies and publishers to print directories (call books) of licensed operators. DOC maintains a database of the licensees which includes names and addresses.

The operator opposed release of his personal data because he did not want to become the target for "junk" mail or thieves seeking expensive radio equipment.

The complaint influenced DOC to put on hold release of the information pending the Privacy Commissioner's decision. This prompted a barrage of calls and letters from operators to both DOC and the Commissioner's office.

The investigation found that DOC release of the information is a complicated issue. DOC officials told the Commissioner why the department considers the release "consistent with" the purpose for its collection.

DOC explained that it is responsible for managing the radio spectrum, a limited public resource. Individuals who pass the examinations are assigned a call signal and are licensed to use a portion of the public air waves. Publicly identifying these operators allows them to police themselves since misuse by amateurs can interfere with other radio transmission. As radio saturation and electro-magnetic interference grows, DOC considers this policing an important part of spectrum management. DOC also argued that it was not sound public policy to allow individuals to enjoy a shared resource with anonymity.

As a member of the International Telecommunication Union, DOC is obligated to provide public access to names, addresses and call signs under two articles of international regulations which deal with investigating interference, communication amongst operators and their self-training.

As well, DOC discloses licensing information to permit communication amongst amateurs, including verifying signals and technical details. This helps operators who are required by the radio regulations to confirm that a contact is a licensed amateur. DOC is also required to release the names and licence status of amateurs using shared systems (such as satellites) which are funded and maintained by the amateur community.

DOC agreed that not all operators want to join clubs, volunteer for emergency communications services or be listed in call books. However, it considered that amateurs may not opt out of their responsibility to make public their use of the airwaves.

The Commissioner accepted DOC's strong case for disclosure and noted that operators may ask private call book publishers not to list their information. He considered the complaint not well-founded.

Solicitor-client privilege widely drawn

A woman involved in a wrongful dismissal suit against Transport Canada applied for her information in its 20 standard employee banks. Her complaint alleged slow response and the withholding of material.

The investigation found that there was no information about the woman in 14 of the banks. It was also evident that information had been withheld from the grievance file, some because it concerned another person and some because the department considered that it was protected by solicitor-client privilege.

The investigator found that Transport Canada had exempted the request for its lawyer's opinion, the opinion itself, and all the background material. This material — part of the regular grievance file — was withheld in order to seek a legal opinion. The department held that once this information was attached to the request for legal advice, it became privileged.

However, legal precedents are clear that solicitor-client privilege covers communications between the parties and materials created or obtained specifically for litigation. All documents given by a client to a legal adviser are not privileged. For example, when facts are obtained from other sources, not for or by legal counsel, they are not privileged.

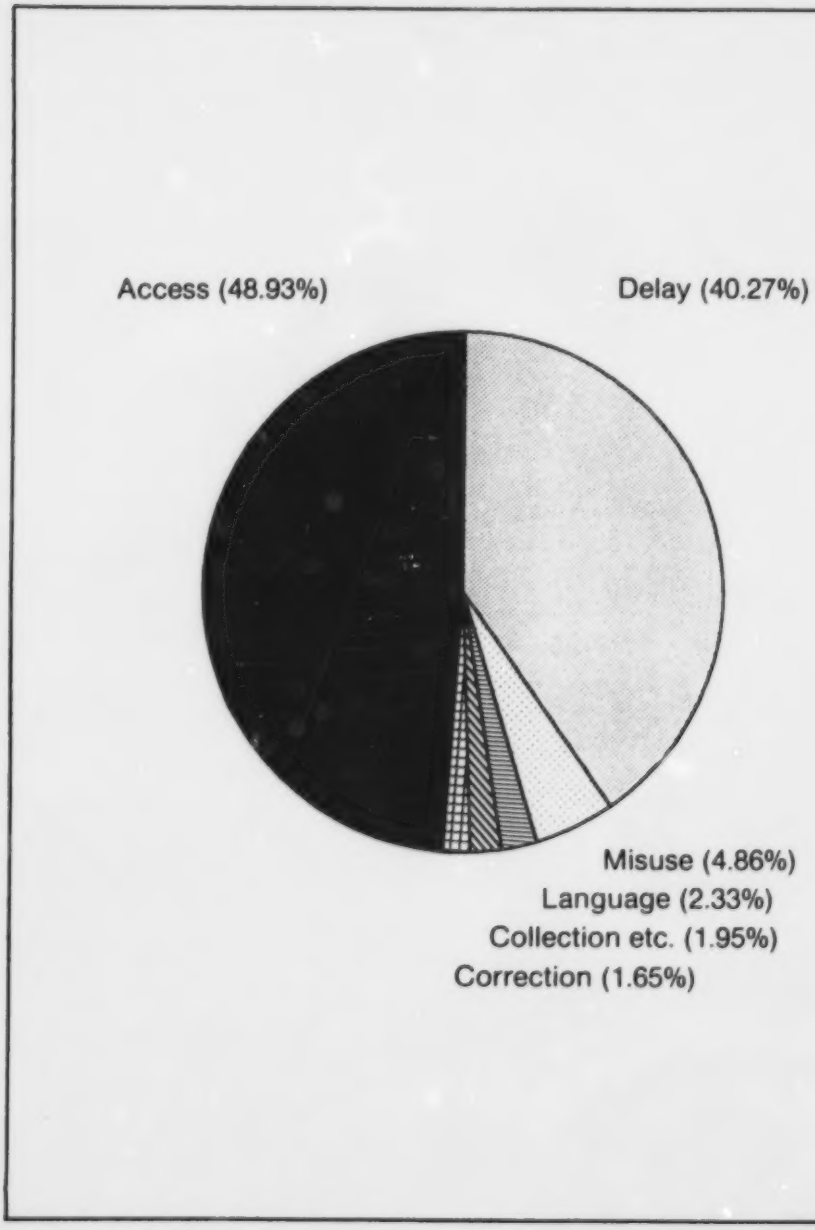
The Commissioner advised Transport Canada that he considered its view "extends unacceptably the concept of privilege". His recommendation to release the grievance file material prompted the department into partial release of the information. The Commissioner proposed to the complainant that he take her case to the Federal Court. She agreed and the Commissioner notified the department. In the meantime, Transport Canada had received advice from the Department of Justice and decided to release the material. The Commissioner considers the complaint well-founded.

Completed Complaints by Department, Type and Result

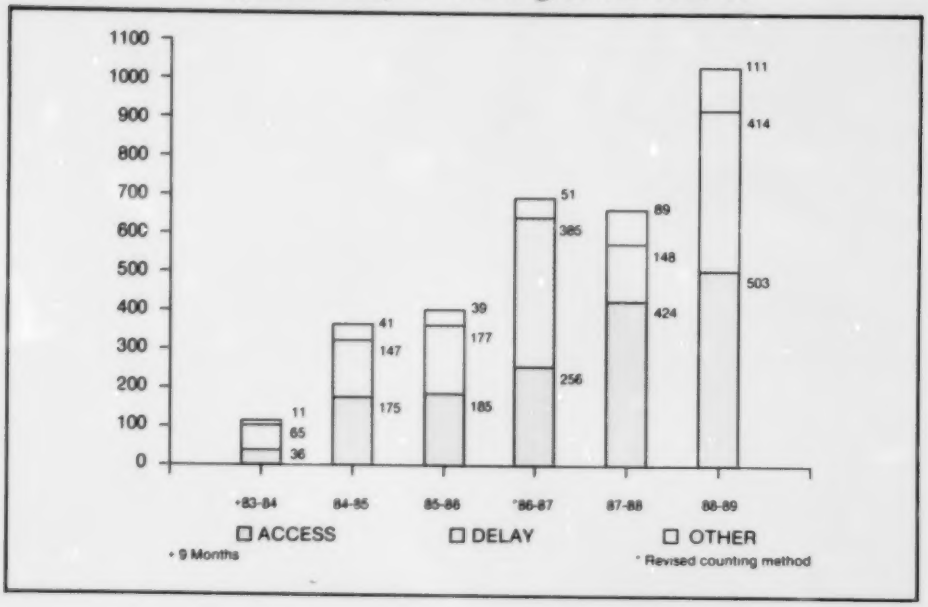
Department	Total	Well-founded	Well-founded - Resolved	Not Well-founded	Dis-continued
Agriculture Canada	5	0	2	3	0
Canada Labour Relations Board	1	0	0	1	0
Canada Mortage and Housing Corporation	1	0	1	0	0
Canada Ports Corporation	4	0	4	0	0
Canada Post Corporation	12	2	2	7	1
Canadian Human Rights Commission	11	0	2	9	0
Canadian Security Intelligence Service	49	3	6	40	0
Communications, Department of	2	1	1	0	0
Consumer and Corporate Affairs Canada	1	0	0	1	0
Correctional Service Canada	404	203	29	168	4
Employment and Immigration Canada	68	24	13	28	3
Energy, Mines and Resources Canada	2	1	1	0	0
Environment Canada	3	0	0	0	3
External Affairs Canada	14	3	1	10	0
Health and Welfare Canada	18	3	5	8	2
Indian and Northern Affairs Canada	1	0	1	0	0
Justice Canada	5	0	0	5	0
Labour Canada	5	0	0	5	0

Department	Total	Well-founded	Well-founded - Resolved	Not Well-founded	Dis-continued
National Archives of Canada	15	1	0	14	0
National Defence	85	32	4	46	3
National Parole Board	30	3	11	15	1
Office of the Chief Electoral Officer	1	0	0	1	0
Office of the Commissioner of Official Languages	3	0	0	3	0
Office of the Correctional Investigator	1	0	1	0	0
Office of the Inspector General of the Canadian Security Intelligence Service	4	0	0	4	0
Privy Council Office	6	0	1	5	0
Public Service Commission	8	0	4	3	1
Public Works Canada	2	0	0	2	0
Revenue Canada - Customs and Excise	15	5	1	9	0
Revenue Canada - Taxation	37	11	0	21	5
Royal Canadian Mounted Police	109	13	6	86	4
Security Intelligence Review Committee	4	0	0	4	0
Solicitor General Canada	22	0	0	22	0
Transport Canada	77	31	2	43	1
Veterans' Affairs Canada	3	0	0	3	0
TOTAL	**1028**	**336**	**98**	**566**	**28**

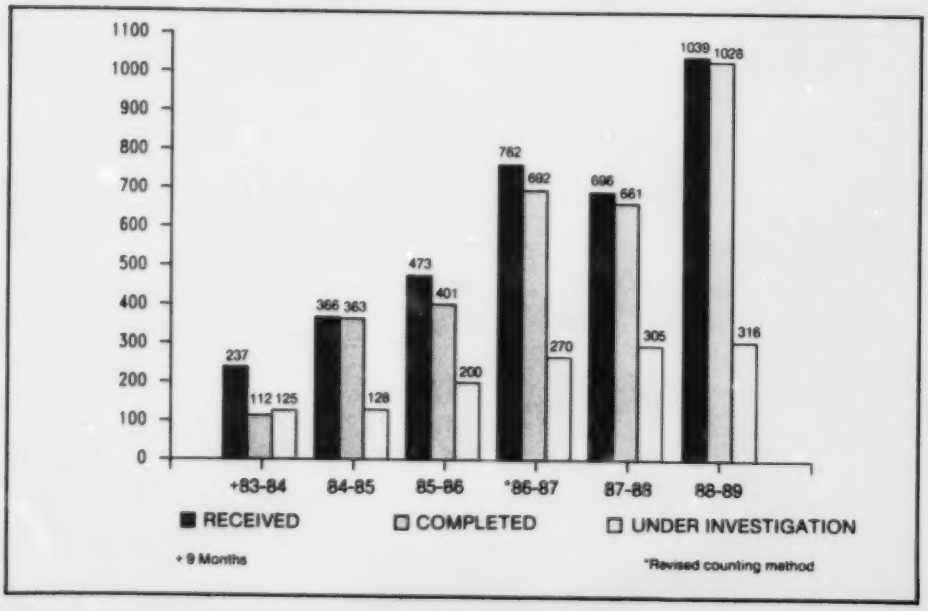
Caseload by grounds 1988-89



Completed complaints and grounds 1983-89



Completed complaints 1983-89



Inquiries

Inquiries to the Privacy Commissioner's office almost doubled in this fiscal year as the staff dealt with 2,041 compared to 1,248 in the previous year. The office now has a full-time inquiries officer who handles the majority of the calls. Her improved system of logging all inquiries makes the increase appear greater than it actually is. Before this, many calls were simply not included as staff members fielded them but lacked the time to officially record them.

Queries cover a broad range. They can be as simple as forwarding an application to see personal information to the proper department (approximately eight per cent of inquiries).

They can also be as time-consuming (but ultimately satisfying) as following up an MP's call about a detailed questionnaire which temporary helpers at Canada Post had to complete before they were hired to deliver advertising mail. Canada Post, after discussion with this office, stopped using the questionnaire. Calls about using and interpreting the *Privacy Act* make up 46 per cent of the inquiries.

Questions and complaints about the use of social insurance numbers climbed to 21 per cent of all inquiries during the year, due in large part to an amendment to the *Income Tax Act* which requires everyone to give their SIN to their financial institutions. Some callers were incensed at the apparent contradiction between the government's newly-announced policy on restricting the number and a requirement to put the SIN in the hands of their bank, trust company, credit union, caisse populaire and stockbroker. Callers were also being told they had to give it to real estate agents (who were banking deposit cheques) and to insurance agents.

Other callers were disturbed at what they considered the "secrecy" with which the new requirement was introduced. In fact, as noted earlier, the amendments to the *Income Tax Act* went through normal Parliamentary procedures. MPs did not query the new SIN requirements and the media did not report them. Most callers discovered the new law, which imposes a fine for failure to produce the SIN, when they bought the new series of Canada Savings Bonds or went to the bank. They were not amused.

About ten per cent of callers are concerned about federal agencies that are not subject to the *Privacy Act,* often Crown corporations such as Air Canada and Canadian National Railways. Some Crown corporations are expected to be covered by the Act in 1989.

Fifteen per cent of the calls concerned privacy issues in either the provincial or private sector and thus were beyond the authority of this office. For example, an Ontario woman called to determine whether the *Privacy Act* would prevent her municipality from selling its voters list to companies or individuals. The office was unable to investigate since municipalities are not covered by the *Privacy Act* and will not be subject to the Ontario legislation until 1991. (Federal enumeration lists, by comparison, may not be sold.)

Compliance Directorate

Who Was Audited

The Commissioner's office again selected audit candidates nominating targets according to overall level of risk measured as objectively as possible.

Selected were Canada Post Corporation, the Secretariat of the Ministry of the Solicitor General and Employment and Immigration Canada. In addition to these major institutions, audits were done on several smaller institutions: the Department of Finance, the Pension Appeals Board, and the Science Council of Canada.

Small agency audits are being concluded in the Law Reform Commission, International Development Research Centre, the Canadian Cultural Property Export Review Board, Export Development Corporation and Canadian Patents and Development Limited.

How and What was Audited

Audits are conducted by teams of two to four investigators who visit selected headquarters units and a number of regional offices. Investigators review a random sample of files from selected information banks and interview managers and staff who use and control the files.

The auditors examine:

* the institution's collection, use, disclosure, retention, disposal and security of personal information;

* the adequacy of internal policies and compliance with central agency policy and guidelines on personal information;

* the accuracy and completeness of listings in the Personal Information Index;

* staff awareness of the *Privacy Act* and its implications for handling personal information;

* individuals' access to their personal information;

* delegation of powers by the department head.

Once the audit is completed, the auditors discuss it with the managers, focussing on any areas of non-compliance. The department first receives summaries of findings, then an audit report. In line with accepted audit practice, the reports address only those areas requiring correction.

Auditing the Auditors

Six auditors cannot in a short time cover all government agencies under the *Privacy Act's* authority. Thus, the Privacy Commissioner has always urged departments' internal auditors to audit for privacy. The year provided encouraging evidence of this happening.

The Canada Employment and Immigration Commission responded. After consulting the Commissioner's office, its internal audit bureau began a review of CEIC's personal information handling. Privacy staff then examined the auditors' working papers to determine the level of reliance they could place on the audit. That review disclosed a thoroughly professional audit which the Privacy Commissioner could accept with as much confidence as if it had been done by his own auditors. (The findings are summarized elsewhere in this section.)

What Was Found

Some findings apply to all of the agencies audited. For example, few employees outside of the access to information and privacy units know about their rights under the *Privacy Act* or understand their responsibilities for the proper collection, retention, use, disclosure and disposal of personal information.

Inadequate protection of personal information is another common finding. Operational (and even some security) staff do not yet fully understand the new government security policy, particularly those sections which deal with the protection of personal information. Nevertheless, auditors found no indications that personal information had been compromised.

Auditors again found personal information holdings that had not been identified or properly described in the *Personal Information Index*. Similarly, some uses of personal information which the institution considered "consistent" with the purpose for the original collection, were not included in the Index descriptions.

The audits underscored the need for a government-wide policy covering who may see personnel files. Such policy should consider the subtleties of the *Privacy Act* and limit the amount of personnel information managers need for discharging the legitimate demands of their positions. The current organization of most personnel files precludes segregating the information according to the "need to know" principle.

Security and Privacy

Most staff treat information security as the domain of security officers or management information specialists. Both of these groups are trained to think of security in terms of classification in the "national interest", not individual privacy. They are often not prepared to deal with the designation "protected", which now applies to all information which is personal but not in the national interest.

Treasury Board, the Communications Security Establishment, the RCMP and the Privacy Commissioner's staff have taken major steps toward creating staff awareness about the protection of personal information. Until now, this information has often not been considered as security sensitive.

Continuing consultation among these organizations has produced levels of protection that match the sensitivity of the personal information. These levels will be included in the government's security policy statement. The publication and application of this new policy should help departments realize security standards for all designated information.

Incident investigations

The office investigated one lost document incident during the year and maintained a watching brief over another department's investigation of missing records. The investigation concerned the loss of tax microfiche from the Calgary district office of Revenue Canada, Taxation. Revenue Canada told the Privacy Commissioner in October 1988 that it had lost 38 sheets out of a set of microfiche. The sheets identified employers (by code number only) and their employees by surname, initials, social insurance number, earnings, pension, unemployment insurance contributions and other deductions. Each fiche (or sheet) could contain data on more than 8,000 individuals.

The investigation began at the Ottawa Head Office. Investigators followed the procedure for producing and shipping microfiche sets and were convinced that the set would have arrived intact at its destination.

Investigators followed the fiche's trail at the Calgary District Office. Once the fiche had been opened and counted, they were put in a holding tray where they were available during the day to approximately 150 staff. At night they were locked in a cabinet, but the keys were kept in an unlocked desk drawer. The first employee who needed the set in the morning could unlock the cabinet and put the fiche in the tray. It was never determined who put out the set on the day the loss was discovered. The 38 fiche were never recovered.

It became apparent that employees could remove fiche from the set and take them to other parts of the floor without completing a log. Only employees from outside that work area were required to log out fiche.

The investigators considered that Revenue Canada's security was adequate for the production and distribution of the microfiche and that staff are highly security conscious. However, once inside a secure area, employees appeared to overlook the need to protect personal information as evidenced by the cabinet key in an unlocked desk drawer. Employees also knew little or nothing about the *Privacy Act* and the obligations it imposes on employees handling personal information.

Following the incident, the office instituted new strict procedures. The set of fiche and readers are now kept and used in a secure room which is staffed while open. Sheets must be logged as used and the set then returned to a locking cabinet. Stringent controls are now in place for destruction of old fiche.

These new controls make redundant any recommendations to increase security in the Calgary unit. However, the Commissioner recommended that other locations review their storage and microfiche handling to ensure compliance with both the *Privacy Act* and the new government security policy. As well, several recommendations made after the previous microfiche theft (Annual Report 1986-87) from the Toronto office were repeated:

* employees should be made aware of their obligations to protect personal information under the *Privacy Act*;

* microfiche should be given even more stringent protection than paper files and

* staff should have access to microfiche only as they need to know.

In the second incident, Correctional Service Canada lost more than 30 boxes of outdated inmate files which were being shipped to the National Archives Records Centre in British Columbia. After almost two weeks of searching, the trucking company found the boxes in its warehouse. There was no evidence that the boxes had been opened. However, standard security precautions could have prevented the incident.

The Audits

Two of this year's audits revealed a potential glitch which generated discussion between the Commissioner's office and the organizations being audited. Canada Post and the Export Development Corporation (both Crown corporations) are subject to the *Privacy Act* but technically are not bound by the federal government security policy. Both corporations have opted into the national interest provisions of the policy, but objected to the office using it as a standard against which to measure their physical security.

The Commissioner does not believe that Crown corporations should be bound necessarily by the policy but considers the government standards a reasonable measurement against which to assess the corporations' security.

Canada Post

The auditors travelled to Ottawa Head Office and divisional headquarters in Edmonton, London, and Quebec City.

Findings

Staff Awareness: As in most government institutions audited, the staff did not understand their own or others' privacy rights, nor their responsibilities under the *Privacy Act*. Canada Post publishes periodic reminders in its internal bulletins, but most staff could not recall such material. Thus, either the information is not distributed widely enough or it is simply having little impact.

Canada Post plans a communications program to support its corporate policy on the protection of personal information.

Personal Information Index Descriptions:

1.) The description of two Human Rights banks (CPC/P-PU-096 and P-PE-809) contained no reference to personal harassment cases found in the files. The bank description will be changed to incorporate a reference to the material.

2.) Change of address cards are now described as being a "class" of personal information. However, the *Privacy Act* requires that personal information used for an administrative purpose be included in an information "bank". Since the cards are used to redirect customers' mail (an administrative purpose) Canada Post will create a new bank to contain address change notices. A second bank has been established (CPC/P-PU-120) for requests from other departments to find individuals who owe Crown debts.

Protection of personal information: Divisional headquarters employees who want to review their personnel files must apply through their supervisors and then examine the files in their presence. This means supervisors have access to all personal information in an employee's file—including such details as medical history, charitable contributions and marriages. This information is unnecessary to supervision. Canada Post will review and correct its access procedures.

Some headquarters personnel files contained limited information on other employees, usually in lists containing names and social insurance numbers. Information about third parties will be removed as the files are drawn and used.

In Edmonton, auditors found waste paper containing personal information being sent for disposal to a private company where it was stored outside and unsecured. Canada Post will ask National Archives to provide secure disposal of sensitive waste wherever possible. Elsewhere it will dispose of its own material.

The auditors also found problems with disposal of other waste materials and control of cabinets or rooms containing personal files. Canada Post is committed to correcting these problems when it implements its new privacy and security policies.

At Ottawa and Edmonton, personal information from the Risk Management Claims bank is shared with private insurance adjusters. However, no formal agreement exists with the company to ensure protection of information according to the *Privacy Act*. Canada Post will obtain insurance adjusters' undertakings to meet both the spirit and intent of the act. It will also determine whether Canada Post should incorporate privacy and security provisions in contracts with all agents collecting or receiving personal information on its behalf.

Improper use of personal information: Investigators found a human rights training manual which included actual grievance files, complaints and investigation reports. The documents have now been made anonymous.

Improper disclosure of personal information: Canada Post shared on one occasion its mailing list of stamp collecting customers with the Royal Canadian Mint "and other reputable mailers". Canada Post considered this a "consistent use" of the information. The Commissioner did not see a reasonable connection between collecting stamps and collecting coins or other items. The exchange has already been stopped.

Retention and Disposal Schedules: Auditors made several recommendations about storage or disposal of personal records that were being kept either too long, or not long enough (the act requires personal information be kept at least two years). Canada Post will take action on each of the recommendations.

Finally, auditors found fingerprints in personnel files in each division they visited. Apparently Canada Post once took fingerprints routinely from all employees. The Commissioner suggested that prints no longer needed should be returned to the individuals. Those still needed might better be stored in security clearance or reliability check files.

Pension Appeals Board

The Pension Appeals Board hears appeals against decisions of the Canada Pension Plan and the Quebec Pension Plan. All the files are held in Ottawa and all personal information is on paper. There are no EDP files.

Findings

Awareness: Board staff knew little about the *Privacy Act*. Management will provide the necessary training.

Personal Information Index Descriptions: The Index incorrectly says that the *Privacy Act* does not apply to any material the board holds about appeals under the Quebec Pension Plan. All personal information under the board's control is subject to the *Privacy Act* and the board will remove the statement from the listing.

Auditors found that the Employee Records bank (PAB/P-PE-801) is held and controlled by Health and Welfare Canada (HWC), and not the board. The description will be moved to HWC's listing and a statement included under the board's listing directing employees to Health and Welfare. The board also intends to create a bank called "Staff Matters" in which it will hold routine staff material.

Protection of Personal Information: During the audit investigators found keys left in the locks of cabinets containing completed files. The cabinets are in the main office and accessible to cleaning staff during the evening. The Board will ensure that keys are removed. Investigators also recommended new destruction procedures for sensitive waste.

Retention and Disposal: There is no retention and disposal schedule for appeals files, some of which date from 1967. The Board will seek National Archives advice on establishing a proper schedule.

Collection of Personal Information: Investigators found that the board receives all Canada Pension Plan Review Committee decisions and supporting evidence, whether or not an appeal has been filed. When there is no appeal, the board returns the evidence, but retains the decision. The Commissioner considers this to be collection of information outside the mandate of the board. The board will change its process for examining review committee files.

Science Council of Canada

The Science Council of Canada assesses Canada's scientific and technological resources, needs and potential and has a mandate to increase public awareness about science and technology.

All files are kept in the Council's office in Ottawa. No personal information is stored electronically or on microfiche.

Findings

Awareness: Science Council staff were generally aware of privacy principles — a rare finding among government institutions. In fact, the Council has conducted research into privacy-related matters.

Security of Personal Information: Auditors found staff members who handle personal information have not been checked for reliability, as required by the government security policy. The Council undertook to screen all employees who use protected information.

Cleaning staff is allowed into the personnel office unescorted after hours. No one checks to ensure that the door is locked after cleaners leave. The Council will instruct commissionaires to make such checks.

Index Bank Descriptions: Two groups of files containing personal information about contract personnel and Council members are not described in the Personal Information Index. The Council will describe these holdings in the next edition of the Index.

Department of Finance

The department implements financial and economic policies and programs. Its offices and some 800 employees are in Ottawa.

Findings

Awareness: Once again, employees interviewed demonstrated little knowledge of the *Privacy Act*, though the department developed procedures on the Act in 1983 and has since provided periodic briefings. Management is developing new procedures and guidelines which will be distributed to the administrative branch and the office of each assistant deputy minister.

Protection of Personal Information: Auditors found that both supervisors and official languages training staff who had no real need to know were able to review complete personnel files. Moreover, some files contained limited information about other employees. One of the files examined contained a derogatory assessment of another employee.

The department is determining how it could sever sensitive information from these files without hindering supervisors and language staff from discharging their responsibilities.

Keys to cabinets were kept in unlocked drawers in nearby desks and waste personal information was found in regular garbage cans or recyclable-paper bins.

The keys will now be kept personally by the responsible staff member and "burn" bags will be provided for disposal of personal information.

Investigators suggested that the cabinet and room containing records of requests under the *Access to Information Act* and *Privacy Act* be locked when unattended. The department agreed.

Personal Information Index Descriptions: The department maintains records from reliability checks on its employees but does not list the information in the *Personal Information Index*. This effectively prevents employees from asking to see the information since they may not realize it is available.

Treasury Board has amended the description of this bank (one of the standard banks kept by all departments). The department will use Treasury Board's description.

Ministry of the Solicitor General—Secretariat

The Secretariat supports the Solicitor General whose responsibilities include the Royal Canadian Mounted Police, Canadian Security Intelligence Service, Correctional Service of Canada and the National Parole Board. Auditors visited the Secretariat's head office in Ottawa.

Findings

Protection of Personal Information: Auditors found many of the same deficiencies identified in other agencies: detailed personnel files available to supervisors; lists of employees, some with social insurance numbers, in others' personnel files; files in locked cabinets—but keys in nearby unlocked desk drawers; personal information in regular garbage and cabinets left unlocked when offices are not staffed. As well, file covers for records in the Employee Personnel Record bank had neither a security classification nor "Protected" designation.

The Secretariat agreed to examine the problem of limiting access to personnel files. It will also remind staff about their security responsibilities. "Protected" folders are now used for new personnel files (or when requested) though the secretariat does not consider it feasible to convert all existing files.

Personnel files containing sensitive personal information should be marked appropriately because the investigation found that some information had been revealed "outside the organization that created or collected it".

Although the Secretariat has an adequate security procedure, investigators witnessed the offices left open and unstaffed.

Improper Use of Personal Information: A human resources desk manual uses, as examples, copies of actual completed forms and memoranda. The material identifies individuals. Management agreed to remove the identifying information.

Retention and Disposal of Personal Information: Employee personnel records and RCMP personnel and administrative records were retained beyond the approved period. The National Security Records bank (P-PU-026) had no disposal schedule. The Secretariat agreed to review personnel files annually and consult with National Archives and the Canadian Security Intelligence Service on disposal of the other files.

Personal Information Index Descriptions: Records of employee reliability checks are included in the secretariat's Security Clearances bank (P-SE-909) but are not described. Several banks have a National Archives approval number without the listing describing how long information is kept. Reliability checks will be included in the new standard bank created by Treasury Board. This bank, and disposal schedules for other banks, will be described in the next edition of the Index.

An Old Issue: In 1986 the deputy solicitor general agreed to purge personal information from the files in one of the secretariat's banks, Protection of Privacy (P-PU-035). The bank was then to be removed from the Index. During the audit, investigators found that the bank continues to be listed and only 200 of the 600 files have been purged. The Secretariat has assured the Commissioner that the task will be completed by September 1989.

Employment and Immigration Canada (EIC)

The Internal Audit

This audit was divided into two parts . The first was done by EIC's own internal audit bureau and focussed on protection of personal information about EIC clients. The Privacy Commissioner's role was to "audit the auditors". During the next two years the internal audit bureau will examine its personnel information banks and information in EDP files.

The second part, conducted by the Privacy Commissioner's office, was of EIC's Employee Assistance Program (EAP) files.

The internal audit's objective was broader in scope than those done by privacy auditors because EIC assessed the effectiveness of its internal administration and structures in dealing with both the *Privacy Act* and the *Access to Information Act*.

In an internal audit the Commissioner provides overall advice, when needed, and comments or makes recommendations on the department's compliance with the *Privacy Act's* rules concerning collecting, using, maintaining, disclosing and disposing of personal information.

Employment and Immigration, one of the largest federal government departments, provides employment counselling, training and referrals to millions of Canadians, administering the Unemployment Insurance Plan and screening and providing services to immigrants.

"The need for privacy protection is obvious. The whole of EIC, with its 800 offices, is a veritable repository of personal information. EIC runs on personal information", concluded the internal audit report. The Privacy Commissioner couldn't have put it better.

Findings

Staff Awareness: EIC auditors found privacy coordinators knowledgeable about the *Privacy Act* but other staff were not as well informed. As a result, there were inconsistencies in handling informal requests or requests from third parties such as provincial governments or advocacy groups. EIC has given priority to producing operational manuals for staff and will supplement these with training throughout the department.

Collection and Use of Information: The auditors found that a number of forms which collect personal information contain incomplete references to the *Privacy Act*. They suggested improving the privacy notice on the forms by adding descriptions of the data and listing the ways it is used, the bank in which it is kept and the organizations with which it is shared. They also recommended improving the description of the Unemployment Insurance Claim File bank in the Personal Information Index because it may not adequately describe all of the data in the files.

To ensure that its forms comply with the *Privacy Act*, EIC will ask program staff to refer forms which collect personal information to the Public Rights Administration Directorate for advice.

Data Matching: EIC shares (or matches) more information with other agencies than perhaps any other federal department. Matches include comparisons with Revenue Canada, Taxation data to ensure that individuals are reporting earnings and that those collecting unemployment insurance are not also working. The matches are carried out under the *Unemployment Insurance Act* and the *Immigration Act*.

The *Privacy Act* also allows matching by "an agreement or arrangement" between government agencies and with other governments, whether Canadian or international, in order to administer or enforce a law or carry out an investigation.

The internal auditors found that not all matches are governed by written agreements and that a portion of the agreements have been in effect too long to reflect current legislation. Without formal agreements, staff have insufficient guidance on what information can be shared and how it can be used. The auditors recommended providing summaries of agreements to operational staff, completing all pending agreements and then conducting a follow-up audit to ensure that EIC complies with the new Treasury Board data matching policy.

EIC will review all agreements and complete those still being considered. As well, it will report all current data matches to the Privacy Commissioner and ensure that they all are listed in the *Personal Information Index*. (The new Treasury Board matching policy requires all departments to advise the Privacy Commissioner's office 60 days ahead of any new matches.)

Security: EIC auditors found that some service contracts with private companies do not contain privacy or security clauses, meaning that the companies may not always treat personal data in confidence. Auditors cited examples of companies or individuals providing services such as transportation, document shredding, office cleaning (particularly in offices with open shelving), interpretation, transcription, EDP and psychological diagnosis.

Auditors recommended revising regional contracts to include clauses to protect personal information according to the requirements of the *Privacy Act*, the security policy and EIC's own regulations.

Disposal of personal information: Clearly there was no consistent disposal of waste personal documents among EIC offices. Auditors found that some sorted waste for shredding or regular garbage; others simply put it out with disposable material from other building tenants. Since local office staff estimate that as much as 90 per cent of waste is personal information, auditors questioned the need to sort. The auditors also found that no single unit ensures that all microfiche are accounted for and eventually destroyed. The procedures varied from sending old fiche to regional offices, regional computer centres or to National Archives. The auditors suggested a standard procedure for eventual destruction of out-of-date fiche.

EIC's Security Task Force will address both the incorporation of security clauses in service contracts and the control and destruction of microfiche in its workplan.

Employee Assistance Files (EAP)

These files are among the most sensitive personal files kept by government, recording personal information of individuals undergoing counselling for health or behavioural problems. The files are seen only by the employee and the counsellor. Theft or unauthorized release could cause the employee irreparable harm.

As a result, auditing EAP files poses its own problems for both the department and the Privacy Commissioner. The Commissioner is torn between needing to ensure that the information is seen by as few as possible but requiring evidence that it is appropriately collected and protected. Thus, the auditor examines randomly selected anonymous files to determine whether the information meets privacy standards for collection, use, retention, disclosure and disposal.

In EIC's case there were no EAP files in the Ottawa office. EIC's policy is to maintain as little information as possible, passing necessary details on to outside counsellors. The decision not to maintain files is understandable, even commendable, as a method of ensuring client confidentiality. But the practice means there is no documentary evidence of uses of the information, nor that the client has consented to its release.

The Commissioner observed that the department has to make a trade-off between restricting the amount of sensitive personal information in files and the need for operational controls. He proposed that EIC re-examine its current procedures.

Auditors made several suggestions for improving physical security of the unit's records and disposal of waste containing personal data. The Commissioner recommended that EIC also make the improvements in the regional offices that kept files.

Notifying the Commissioner

Generally, the *Privacy Act* prohibits federal government agencies from releasing personal information to anyone other than the individual concerned. As with most rules, there are exceptions. In fact, the Act has 13 — from releases to comply with a warrant or subpoena, to helping validate aboriginal peoples' claims or grievances.

Among those exceptions are two which require the government agency to notify the Privacy Commissioner. The first covers releasing information "in the public interest" or to benefit the individual concerned. The notification gives the Commissioner an opportunity to advise the individual of the release if that is considered necessary. The second exception deals with releases for a use "consistent" with the purpose for which it was originally collected (but not described in the *Personal Information Index*).

The *Privacy Act* does not provide a means for the Commissioner or the individual to block release. The *Access to Information Act* gives third parties the right to court action to prevent the release of corporate information. The Privacy Commissioner believes that individuals too should be able to prevent the release of what they consider to be unwarranted and damaging release.

There were early suspicions that these exceptions to the general rule prohibiting the disclosure of personal information to third parties would prove to be the *Privacy Act* "Mack truck" clause. It was feared that there would be a full-scale release of personal information based on broad interpretations of "public interest" and "consistent" use. To prevent such abuse, the Commissioner itemized all uses of these releases in his annual report.

So far no abuse has been evident. While the office continues to examine each notification, beginning this year, only global statistics and select examples for illustrative purposes are reported. A detailed breakdown of the 24 notifications can be obtained from the Privacy Commissioner's office.

The MPs — again

Once again Employment and Immigration Canada (EIC) advised the Privacy Commissioner how it would handle MPs' requests for personal information about constituents during the federal election campaign.

The *Privacy Act* allows government agencies to release personal information to an MP who is trying to help solve a constituent's problem. Once Parliament is dissolved, however, MPs have only the status of ordinary citizens. This means, according to the letter of the law, that MPs may no longer (without the individual's consent) inquire on behalf of a constituent about foul-ups with a government agency since this would require them to see personal information.

It seems doctrinaire to impede MPs seeking to help constituents while in the legal limbo of an election period. On the other hand, other candidates may feel unfairly disadvantaged due to the incumbent's special access to government information. EIC — the department most affected — advised the Privacy Commissioner that during the election period it would once again release information without consent to former MPs since it "would clearly benefit" the person concerned [paragraph 8(2)(m)(ii)].

The Privacy Commissioner agreed to the solution — the same one used during the 1984 election. But he repeated his concern that delegating the discretion to disclose personal information to "any" EIC officer or employee increased the opportunity for abuse. Privacy staff reviewed 1479 such notifications during the election campaign.

The *Privacy Act* should be amended before the next election to clarify whether, during an election period, incumbent MPs should maintain their special access to government information when helping a constituent.

Breach of dog's quarantine period

Canada Post advised the Privacy Commissioner that it had given an Agriculture Canada veterinarian the address change of a woman who appeared to have breached her dog's six-month quarantine period. The dog had been in contact with a rabid animal and had not completed the required treatment.

The post office reached the woman directly but she did not cooperate. Although the *Animal Disease and Protection Act* does not authorize release of the information, Canada Post concluded the disclosure was in the public interest. The Commissioner did not question the release.

Inmates' names and addresses to Chief Electoral Officer

Following a Manitoba Court decision that inmates had the right to vote in the federal election, Correctional Service Canada advised the Commissioner that it would give the names and addresses of all federal inmates in Manitoba to the Chief Electoral Officer of Canada.

The list was to be used by returns officers to organize the voting in penitentiaries and was not to be given to anyone else. However, since the court decision was appealed, the inmates were not enumerated and the list was not sent.

Soviet government alerted to visitor with TB

External Affairs advised the Privacy Commissioner that it had notified Soviet public health authorities about a Canadian visitor with an infectious disease.

Health and Welfare Canada had warned External Affairs that a woman with pulmonary tuberculosis had refused medication and checked herself out of the hospital. She then travelled to the Soviet Union to visit relatives. After calling the Privacy Commissioner's office, External informed the Canadian embassy in Moscow which, in turn, notified the Soviets.

The notification was considered "in the public interest".

Spreading the Word

It has been said that if there were a privacy constituency in Canada — a group of knowledgeable, committed privacy activists — it would fit in the Privacy Commissioner's boardroom (a snug fit even for the Commissioner's own staff).

The job is no longer so lonely. In fact, two recent conferences on privacy (and access to information) filled large meeting rooms in Toronto and Ottawa hotels. A loose network of federal, provincial and unaligned privacy advocates is emerging, allied with committed records and EDP systems managers to spread the word.

The public may still be puzzled when told of a *Privacy Act* (and find it faintly hilarious that there is a Privacy Commissioner). Nevertheless, people understand the issues and find them deadly serious.

The Commissioner and his staff welcome opportunities to discuss the Act and the issues. During the year the Commissioner completed a series of some 20 speeches to Canadian Clubs across the country, spoke to (among others) trainee intelligence officers, data processors, heads of federal government agencies and middle level financial managers. He also participated in a Canadian Chamber of Commerce briefing on the implications for the private sector of privacy legislation and the OECD guidelines; and on AIDS at a National Parole Board seminar.

The Commissioner began a series of visits to federal penitentiaries to discuss the *Privacy Act* with staff and inmates. So far he has visited the Prison for Women in Kingston and the medium security institution at Springhill, Nova Scotia.

The Commissioner's staff continues to brief participants on the government's management training courses and spoke to Coast Guard staff in Halifax, a race relations seminar in Montreal, and college classes in Toronto and Ottawa.

The office produced an information package entitled "Do you need help using the *Privacy Act*?" It includes a poster, bookmark and an explanatory brochure describing the Commissioner's role and how to use the office's services.

Corporate Management

Corporate Management provides both the Information and Privacy Commissioners with financial, personnel, administrative, data processing and library services.

Finance

The Offices' total resources for the 1988-89 fiscal year were $5,074,000 and 69 person-years, an increase of $1,152,000 and 11 person-years over 1987-88. Personnel costs of $3,837,201 and professional and special services expenditures of $702,567 accounted for more than 88 per cent of expenditures. The remaining $603,137 covered all other expenses.

Personnel

A substantial increase in person-years for the Privacy Commissioner produced a very active personnel program. New positions were classified and there were 42 staffing actions including two senior management appointments. In addition, the offices underwent a biennial classification audit by Treasury Board and the PM (program management) and IS (information services) positions were reviewed in line with the new classification standards.

The following are the Offices' expenditures for the period of April 1, 1988, to March 31, 1989.

	Information	Privacy	Corporate Management	Total
Salaries	$ 1,268,673	$1,469,048	$568,480	$3,306,201
Employee Benefit Plan Contributions	202,500	246,600	81,900	531,000
Transportation and Communication	29,363	66,204	118,094	213,661
Information	57,681	38,815	1,526	98,022
Professional and Special Services	506,936	144,959	50,672	702,567
Rentals	2,898	64	5,294	18,256
Purchased Repair and Maintenance	1,337	5,112	21,940	28,389
Utilities, Materials and Supplies	9,957	14,738	37,264	61,959
Acquisition of Machinery and Equipment	43,232	85,986	48,464	177,682
Other Payments	1,630	1,569	1,969	5,168
TOTAL	**$2,124,207**	**$2,073,095**	**$ 945,603**	**$5,142,905**

Administration

The offices moved to the 3rd and 4th floors of Tower B, Place de Ville. Improved security measures were implemented for the new premises and a security manual was prepared. In addition, National Archives completed a records management audit.

Informatics

A review of informatics was undertaken with the assistance of outside consultants. The office will implement the major recommendations of the study concerning renewal of the case management system and expansion of report and text production facilities.

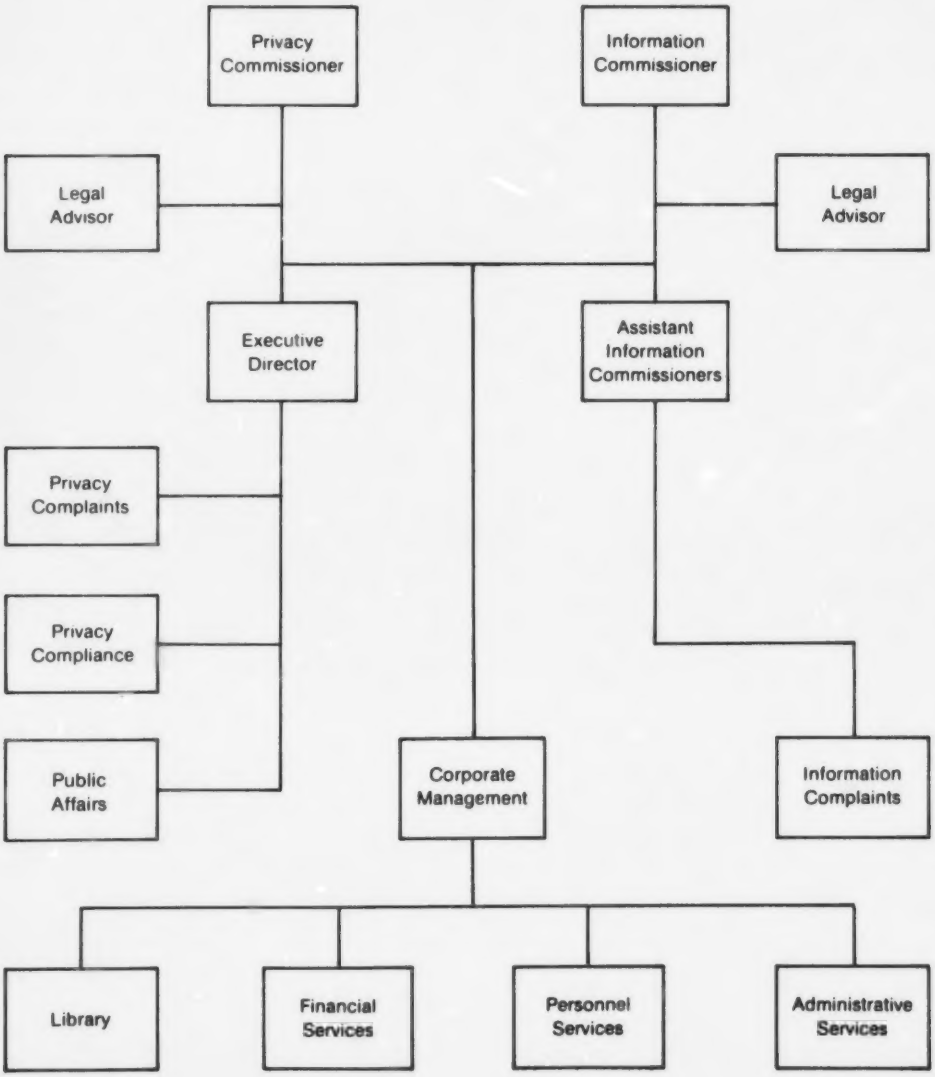
Library

The library continues to provide an information and referral service for both Commissioners. It offers a full range of library services, including interlibrary loan, automated reference, and literature searches.

Last year, approximately 500 publications about access to information, the protection of privacy and the ombudsman function were added to the library's inventory. The public is welcome to consult our collection, which also includes newspaper clipping files, periodicals, and annual reports.

Appendix I

Offices of the
Information and Privacy
Commissioners of Canada



Appendix II

Government Institutions Covered by the Act

Advisory Council on the Status of Women

Agricultural Products Board

Agricultural Stabilization Board

Agriculture Canada

Atlantic Development Council

Atlantic Pilotage Authority

Atomic Energy Control Board

Bank of Canada

Bilingual Districts Advisory Board

Board of Trustees of the Queen Elizabeth II Canadian Fund to Aid in Research on the Diseases of Children

Bureau of Pension Advocates

Canada Council

Canada Deposit Insurance Corporation

Canada Employment and Immigration Commission

Canada Labour Relations Board

Canada Lands Company Limited

Canada Mortgage and Housing Corporation

Canada-Newfoundland Offshore Petroleum Board

Canada-Nova Scotia Offshore Petroleum Board

Canada Ports Corporation

Canada Post Corporation

Canadian Aviation Safety Board

Canadian Centre for Occupational Health and Safety

Canadian Commercial Corporation

Canadian Cultural Property Export Review Board

Canadian Dairy Commission

Canadian Film Development Corporation

Canadian Government Specifications Board

Canadian Grain Commission

Canadian Human Rights Commission

Canadian Institute for International Peace and Security

Canadian International Development Agency

Canadian International Trade Tribunal

Canadian Livestock Feed Board

Canadian Patents and Development Limited

Canadian Penitentiary Service

Canadian Pension Commission

Canadian Radio-television and Telecommunications Commission

Canadian Saltfish Corporation

Canadian Security Intelligence Service

Canadian Unity Information Office

The Canadian Wheat Board

Communications, Department of

Consumer and Corporate Affairs Canada

Defence Construction (1951) Limited

The Director of Soldier Settlement

The Director, The Veterans' Land Act

Economic Council of Canada

Employment and Immigration Canada

Energy, Mines and Resources Canada

Energy Supplies Allocation Board

Environment Canada

Export Development Corporation

External Affairs Canada

Farm Credit Corporation

Federal Business Development Bank

Federal Mortgage Exchange Corporation

Federal-Provincial Relations Office

Finance, Department of

Fisheries and Oceans Canada

Fisheries Prices Support Board

The Fisheries Research Board Canada

Freshwater Fish Marketing Corporation

Grain Transportation Agency Administrator

Great Lakes Pilotage Authority, Ltd.

Hazardous Materials Information Review Commission

Health and Welfare Canada

Historic Sites and Monuments Board of Canada

Immigration and Refugee Board

Indian and Northern Affairs Canada

International Development Research Centre

Investment Canada

Jacques Cartier and Champlain Bridges Incorporated

Justice Canada

Labour Canada

Laurentian Pilotage Authority

Law Reform Commission of Canada

Medical Research Council

Merchant Seamen Compensation Board

Metric Commission

National Archives of Canada

National Arts Centre Corporation

The National Battlefields Commission

National Capital Commission

National Defence

National Design Council

National Energy Board

National Farm Products Marketing Council

National Film Board

National Library

National Museums of Canada

National Parole Board

National Parole Service

National Research Council of Canada

National Transportation Agency (formerly Canadian Transport Commission)

Natural Sciences and Engineering Research Council

Northern Canada Power Commission

Northern Pipeline Agency

Northwest Territories Water Board

Office of the Auditor General

Office of the Chief Electoral Officer

Office of the Commissioner of Official Languages

Office of the Comptroller General

Office of the Coordinator, Status of Women

Office of the Correctional Investigator

Office of the Custodian of Enemy Property

Office of the Director of Investigation and Research

Office of the Inspector General of the Canadian Security Intelligence Service

Office of Privatization and Regulatory Affairs

Office of the Superintendent of Financial Institutions Canada

Pacific Pilotage Authority

Pension Appeals Board

Pension Review Board

Petroleum Compensation Board

Petroleum Monitoring Agency

Prairie Farm Assistance Administration

Prairie Farm Rehabilitation Administration

Privy Council Office

Public Service Commission

Public Service Staff Relations Board

Public Works Canada

Public Works Land Company Ltd.

Regional Development Incentives Board

Regional Industrial Expansion

Revenue Canada

Royal Canadian Mint

Royal Canadian Mounted Police

Royal Canadian Mounted Police External Review Committee

RCMP Public Complaints Commissioner

The St. Lawrence Seaway Authority

Science and Technology Canada

Science Council of Canada

The Seaway International Bridge Corporation, Ltd.

Secretary of State

Security Intelligence Review Committee

Social Science and Humanities Research Council

Solicitor General Canada

Standards Council of Canada

Statistics Canada

Statute Revision Commission

Supply and Services Canada

Tax Review Board

Transport Canada

Treasury Board Secretariat

Veterans' Affairs Canada

War Veterans Allowance Board

Yukon Territory Water Board

Commissaire à la
protection de la vie privée

Rapport annuel 1988-89

Rapport annuel du Commissaire à la protection de la vie privée 1988-89

Le Commissaire à la protection de la vie privée du Canada
112, rue Kent,
Ottawa (Ontario)
K1A 1H3

(613) 995-2410
1-800-267-0441

© Ministre des Approvisionnements et Services Canada 1989

N° de cat. IP 30-1/1989

ISBN 0-662-56842-7

"Les seuls renseignements personnels que peut recueillir une institution fédérale sont ceux qui ont un lien direct avec ses programmes ou ses activités . . . ".

"Une institution fédérale est tenue de recueillir auprès de l'individu lui-même, chaque fois que possible, les renseignements personnels . . . le concernant . . . ".

" . . . est tenue d'informer l'individu . . . des fins auxquelles ils (les renseignements personnels) sont destinés".

" . . . est tenue de veiller, dans la mesure du possible, à ce que les renseignements personnels . . . soient à jour, exacts et complets".

"À défaut du consentement de l'individu concerné, les renseignements personnels relevant d'une institution fédérale ne peuvent servir à celle-ci :

a) qu'aux fins auxquelles ils ont été recueillis ou préparés . . . "

(ou conformément aux exceptions précises énoncées à l'article 8)

La *Loi sur la protection des renseignements personnels*.

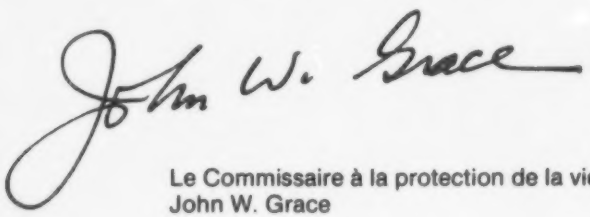
L'honorable Guy Charbonneau
Président
Sénat
Ottawa

le 30 juin 1989

Monsieur Charbonneau,

J'ai l'honneur de soumettre mon rapport annuel au Parlement. Ce rapport couvre la période allant du 1er avril 1988 au 31 mars 1989.

Veuillez agréer l'expression de mes sentiments respectueux.



Le Commissaire à la protection de la vie privée,
John W. Grace

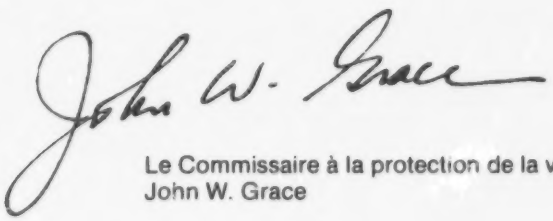
L'honorable John A. Fraser, c.p., c.r., député
Président
Chambre des communes
Ottawa

le 30 juin 1989

Monsieur Fraser,

J'ai l'honneur de soumettre mon rapport annuel au Parlement. Ce rapport couvre la période allant du 1er avril 1988 au 31 mars 1989.

Veuillez agréer l'expression de mes sentiments respectueux.



Le Commissaire à la protection de la vie privée,
John W. Grace

Table des matières

Mandat 1
Des hauts et des bas 2
Mais qui décide? 11
La protection de la vie privée dans le contexte du SIDA 15
À l'aube de l'ère biotechnologique 18
Sécurité informatique 20
Les dossiers du SCRS 22
Qu'est-ce qu'il y a avec le chèque? 24
Direction générale des plaintes 26
Dossiers 28
Demandes de renseignements 37
Direction générale de l'observation 43
- Société canadienne des postes 47
- Commission d'appel des pensions 49
- Conseil des sciences du Canada 50
- Ministère des Finances 51
- Secrétariat du Solliciteur général 52
- Emploi et Immigration Canada (EIC) 53

Aviser le Commissaire 57
Faites passer 60
Gestion intégrée 61
Annexe I 63
Annexe II 64

Mandat

La *Loi sur la protection des renseignements personnels* donne aux individus accès à leurs renseignements personnels détenus par le gouvernement fédéral; protège la vie privée des individus en restreignant le nombre des personnes qui peuvent consulter les renseignements; et donne aux individus un certain contrôle sur la collecte et l'usage des renseignements par le gouvernement.

La Loi énonce les principes des pratiques équitables en matière d'information qui exigent que le gouvernement :

- ne collecte que les renseignements dont il a besoin pour exécuter ses programmes;
- recueille les renseignements directement auprès de l'individu concerné, dans la mesure du possible;
- informe l'individu des fins auxquelles ils sont destinés;
- conserve les renseignements suffisamment longtemps pour en assurer l'accès aux individus; et
- veille « dans la mesure du possible » à ce que les renseignements personnels soient exacts et complets.

Toute personne présente au Canada peut déposer une plainte auprès du Commissaire à la protection de la vie privée si :

- elle s'est vu refuser une partie quelconque des renseignements;
- le droit de demander la correction de certains des renseignements contenus dans le fichier ou de les annoter leur est refusé;
- le ministère prend plus des 30 jours initiaux ou des 60 jours maximums pour fournir les renseignements;
- la description du contenu des fichiers de renseignements donnée dans le Répertoire des renseignements personnels est incorrecte à un quelconque égard;
- la liste donnée dans le Répertoire pour chaque ministère ne décrit pas tous les usages qui sont faits des renseignements personnels;
- une institution recueille, conserve, utilise ou élimine des renseignements personnels d'une manière qui contrevient à la *Loi sur la protection des renseignements personnels*.

Les enquêteurs du Commissaire à la protection de la vie privée examinent tous les fichiers (y compris ceux considérés inconsultables), à l'exception des renseignements confidentiels du Conseil privé de la Reine, pour s'assurer que les institutions fédérales se conforment à la Loi.

La Loi confère également au Commissaire à la protection de la vie privée le pouvoir de vérifier la façon dont les institutions fédérales recueillent, utilisent et éliminent les renseignements personnels, sans devoir attendre qu'une plainte soit déposée.

Des hauts et des bas

Dans notre domaine, l'évaluation des résultats d'un an de travail est entièrement fonction des normes utilisées. Essayer de résumer la situation en quelques formules accrocheuses, c'est risquer de verser dans la fausse représentation, car la question est désormais bien trop complexe.

Même la Cour suprême du Canada a contribué à nuancer les résultats, en déclarant dans *Sa Majesté la Reine* c. *Brandon Roy Dyment* que « la notion de vie privée est essentielle au bien-être de la personne » et que « l'interdiction qui est faite au gouvernement de s'intéresser de trop près à la vie des citoyens touche à l'essence même de l'État démocratique ». Le message ne saurait être plus clair et la source plus digne de foi.

Dans ce jugement, la Cour a renforcé l'opinion qu'elle avait déjà formulée en déclarant que la protection des « particuliers » contre les intrusions injustifiées... dans leur vie privée » est établie par l'article 8 de la Charte canadienne des droits et libertés (« Chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives »). Le jugement rendu dans l'affaire Dyment, rédigé par le juge G.V. La Forest, a aussi posé un principe fondamental, le suivant : « ...si le droit à la vie privée de l'individu doit être protégé, nous ne pouvons pas nous permettre de ne faire valoir ce droit qu'après qu'il a été violé... Il faut empêcher les atteintes au droit à la vie privée et, lorsque d'autres exigences de la société l'emportent sur ce droit, il doit y avoir des règles claires qui énoncent les conditions dans lesquelles il peut être enfreint. »

La *Loi sur la protection des renseignements personnels* est précisément un ensemble de règles comme celles-là. Jusqu'à présent, la Cour suprême a rendu deux décisions qui lui ont donné d'excellentes assises constitutionnelles, en établissant explicitement la protection de la vie privée en vertu de l'article 8 de la Charte.

Le Parlement peut tirer fierté d'être allé plus loin que la Charte et la Cour suprême en établissant dans la *Loi sur la protection des renseignements personnels* les règles régissant les utilisations gouvernementales des renseignements personnels obtenus des citoyens. En ces jours où les différends sont nombreux, le Parlement n'a pas toujours cette longueur d'avance sur les tribunaux.

Et pourtant, le front juridique n'est pas toujours une source de joie sans mélange pour les protecteurs de la vie privée. Ainsi, la décision de la Cour suprême dans *Stewart* c. *Sa Majesté la Reine* semble marquer un recul. Dans cette affaire, la Cour a jugé qu'il est impossible de voler des renseignements confidentiels, parce qu'on ne peut les considérer comme un bien au sens du Code criminel.

L'affaire est connue : un syndicat qui tentait de former une unité de négociation dans un hôtel n'avait pu obtenir les noms et les adresses de quelque 600 employés, parce que la direction considérait ces renseignements comme confidentiels. Un consultant embauché par le syndicat s'est procuré la liste par l'entremise d'un gardien de sécurité qu'il avait soudoyé pour copier les noms d'une liste conservée à l'hôtel, sans en sortir l'original et sans le modifier le moindrement. Le consultant a été accusé au pénal d'avoir incité à commettre une fraude, un vol et un méfait en portant atteinte à la propriété privée de l'hôtel et de ses employés.

La condamnation prononcée par la Cour d'appel de l'Ontario a été renversée à l'unanimité par la Cour suprême. Le juge Antonio Lamer a rédigé la décision de la Cour en concluant que « ...les renseignements confidentiels ne sont pas d'une nature telle qu'ils peuvent être détournés parce que, si l'on s'approprie des renseignements confidentiels sans s'emparer d'un objet matériel, par exemple en mémorisant ou en copiant des renseignements... le prétendu propriétaire ne se voit privé ni de l'usage, ni de la possession de ces renseignements ». Plus loin, le juge a souligné que « ...on ne peut être privé de la confidentialité parce qu'on ne peut pas en être propriétaire ».

Avec tout le respect que nous devons à la Cour, pour imiter la formule rituelle des avocats, force nous est de dire que ces observations ont des implications alarmantes pour la société de l'information en général et pour la *Loi sur la protection des renseignements personnels* en particulier. Si la Loi promet quelque chose, c'est bien de protéger la confidentialité des renseignements personnels recueillis par les institutions gouvernementales. La subtile distinction juridique sur la possibilité ou l'impossibilité pour la confidentialité d'être un bien n'a tout simplement aucune pertinence dans un contexte où il faut préserver la confidentialité de renseignements de nature délicate.

Si cette interprétation de profane de la décision de la Cour est valide, nous devons conclure que la Cour n'a pas accordé suffisamment d'importance au grave préjudice qui pourrait résulter d'un accès non autorisé aux masses énormes de renseignements personnels délicats que détiennent le gouvernement et le secteur privé.

La Cour semblait songer surtout, sinon exclusivement, aux risques de préjudice commercial, mais il est certain que de terribles tragédies personnelles risqueraient de résulter d'une communication non autorisée des dossiers d'enquête de la Gendarmerie royale du Canada, des rapports de surveillance du Service canadien du renseignement de sécurité et des dossiers médicaux de Santé et Bien-être social Canada — et ce ne sont là que des organismes gouvernementaux.

Pourtant, la Cour semble avoir déclaré qu'il est possible de mémoriser, de copier — voire, par implication, de photographier — des documents sans être passible de sanctions pénales, tant qu'on ne s'approprie pas les documents eux-mêmes.

L'affaire *Stewart* c. *Sa Majesté la Reine* n'a pas reçu toute l'attention du public qu'elle méritait. S'il s'était agi de renseignements à caractère délicat sur la santé — ou de dossiers financiers — plutôt que d'une liste de noms de personnes impliquées dans un vulgaire conflit de travail, il y aurait eu une véritable tempête de protestations, et à juste titre.

La *Loi sur la protection des renseignements personnels* ne prévoit pas de sanctions. Jusqu'à ce que la décision de la Cour suprême ait été rendue publique, une condamnation pour vol, en vertu du paragraphe 298(1) du *Code criminel*, ou pour fraude, en vertu du paragraphe 328(1) dudit Code, semblait suffisante comme moyen de dissuasion. Par conséquent, on n'a pas jugé utile que la *Loi sur la protection des renseignements personnels* prévoie elle-même des sanctions. Avec le jugement *Stewart*, la protection du Code criminel s'est envolée.

Il reste bien sûr l'abus de confiance, et c'est en vertu de cette accusation qu'on a pu condamner l'employé de Revenu Canada qui avait volé les dossiers de l'impôt sur le revenu de quelque 16 millions de citoyens dans un bureau de Toronto de Revenu Canada. Toutefois, cette accusation ne tiendrait pas dans les cas où des renseignements personnels et confidentiels seraient pris par quelqu'un qui n'est pas fonctionnaire, ou obtenus frauduleusement d'un fonctionnaire ou d'un élu.

Peu de temps après la publication de la décision rendue dans *Stewart* c. *Sa Majesté la Reine*, le Commissaire a fait état de son inquiétude au ministre de la Justice d'alors, l'honorable Ray Hnatyshyn. Selon le Ministre, le *Code criminel* continuera de dissuader les fonctionnaires de communiquer illégalement des renseignements. M. Hnatyshyn a répété que le gouvernement s'était engagé à modifier la *Loi sur la protection des renseignements personnels* pour créer l'assise juridique des normes de sécurité qui figurent actuellement dans la Politique du gouvernement du Canada sur la sécurité. Le Ministre a souligné les modifications apportées en 1985 aux articles 301.2 et 387(1.1) du *Code criminel*, dans lesquels ont été définies les infractions portant atteinte à l'intégrité des systèmes et des services informatiques, qui protègent les données informatisées, y compris les renseignements personnels.

Pourtant, il reste toujours une brèche que le Parlement devrait combler, parce que le gouvernement conserve d'énormes quantités de renseignements sur support papier et qu'il est impossible d'écarter toute possibilité que des personnes de l'extérieur percent l'écran de sécurité conçu pour les protéger.

La Cour suprême a conclu dans *Stewart* c. *Sa Majesté la Reine* que c'est le Parlement, et non les tribunaux, qui devrait décider quelle protection accorder aux renseignements confidentiels. Le Parlement doit répondre à cet appel à l'action en protégeant l'intégrité de la *Loi sur la protection des renseignements personnels*.

En effet, lorsqu'il a adopté la Loi, le Parlement s'est explicitement engagé envers les Canadiens à respecter la confidentialité des renseignements personnels que le gouvernement détenait à leur égard. Cet engagement, c'est la pierre angulaire de toute la législation sur la protection de la vie privée. S'il est possible de s'approprier des renseignements confidentiels sans avoir à craindre des sanctions parce « qu'on ne peut pas être propriétaire de la confidentialité » la promesse que le Parlement a faite dans la *Loi sur la protection des renseignements personnels* a manifestement perdu une grande partie de sa valeur.

Pouvoir « être propriétaire » de la confidentialité pourrait être bien plus important que de posséder des objets matériels, car ceux-ci peuvent être remplacés, tandis que la confidentialité perdue ne peut être retrouvée. Ce n'est rien de moins qu'une perte de contrôle qui porte un dur coup à la dignité humaine.

Tout ne va pas pour le mieux

Bref, la protection de la vie privée a connu cette année des hauts et des bas à la Cour suprême. Dans l'administration fédérale, c'était la même chose. La façon la plus équitable d'évaluer le rendement du gouvernement, c'est de voir ce qu'il a fait pour respecter les délais qu'il s'est fixés en publiant en 1987 *Les prochaines étapes*, en réponse aux recommandations unanimes du Comité de la Justice et du Solliciteur général. Dans le rapport de l'an dernier, nous avons accueilli ce document si rassurant avec un respect digne de celui qui fut accordé aux Dix Commandements au pied du Mont Sinaï. Nous disions alors que, quand tout cela sera enfin en place, la troisième génération de législation canadienne en matière de protection des renseignements personnels sera « ce qu'il y a de mieux sur le plan international ».

Le gouvernement s'est donné un plan d'action grâce auquel il devait atteindre tous ses objectifs dès la fin de 1988. Il a pris des engagements précis, notamment d'entreprendre immédiatement l'élargissement du mandat de la *Loi sur la protection des renseignements personnels* aux sociétés d'État fédérales et de créer le Répertoire de renseignements personnels (le guide des fichiers gouvernementaux de renseignements personnels) en tant que base de données lisibles à la machine. Les démarches ont commencé, oui, mais après plus d'un an, le gouvernement n'a pas encore respecté ses engagements.

Et ce n'est pas tout. Le gouvernement aurait dû publier au printemps 1988 des directives régissant la consultation avec le Commissaire à la protection de la vie privée sur les questions liées à la protection des données. Les modifications à la Loi, et notamment les assises légales promises des normes de sécurité de l'information, devaient être introduites pour l'automne 1988. Enfin, un programme de sensibilisation du public à la Loi devait être en place pour l'hiver 1988. Aucune de ces dates n'a été respectée; pire encore, on n'avait même pas commencé le 31 mars 1989.

Bien sûr, c'était des dates limites que le gouvernement s'était fixées à lui-même, et il ne faudrait pas le fustiger pour avoir sous-estimé la difficulté de sa tâche, par excès d'enthousiasme. D'ailleurs, il a respecté certains de ses engagements clés, même s'il l'a fait un peu plus tard qu'il l'avait promis. Il semble globalement déterminé à mener sa tâche à bien.

Pourtant, la lenteur et l'erreur sont bien décevantes.

Les 12 prochains mois nous montreront si *Les prochaines étapes* seront plus qu'une métaphore largement vide de sens, et si la démarche qu'elles ont promise ne sera qu'un exercice de pure forme. Dans le labyrinthe de la protection des renseignements personnels, le conseiller de la Reine de *La Traversée du miroir*, de Lewis Carroll, serait le guide rêvé :

> « Ici, voyez-vous, vous devez courir de toutes vos forces pour rester à la même place. Si vous voulez progresser, vous devrez courir au moins deux fois plus vite. »

Deux pas en avant

Dans le rapport de l'année dernière, nous avons félicité le gouvernement pour avoir respecté deux de ses engagements, d'abord en adoptant une nouvelle politique régissant son utilisation du numéro d'assurance sociale (NAS), puis en établissant un nouveau système de contrôle du couplage et de l'interconnexion des données. Malheureusement, la rapidité d'exécution du gouvernement est loin d'être à l'égal de l'enthousiasme du Commissaire à la protection de la vie privée. En effet, bien que les politiques sur le NAS et sur le couplage des données aient été annoncées auparavant, elles n'ont été approuvées qu'en avril 1989, après la fin de l'année qui nous intéresse.

Et pourtant, dans ce cas-ci, il faut bien admettre que mieux vaut tard que jamais. Même avec un an de retard, ce sont deux grands pas en avant. (Les mécanismes de réglementation du couplage des données sont décrits de façon détaillée dans le rapport de l'année dernière.)

Il vaut la peine de revenir sur les restrictions que le gouvernement s'est imposées dans son utilisation du NAS, car c'est le plus important des grands engagements qu'il a respectés. Le président du Conseil du Trésor l'a fort bien dit :

> « Bon nombre de Canadiens se sentent menacés par l'utilisation qu'on fait de leur numéro d'assurance sociale comme moyen d'identification universel. Étant donné l'évolution rapide de l'informatique, ces personnes se préoccupent de plus en plus de ce que le NAS puisse permettre un accès non justifié à des renseignements personnels et menace de ce fait leur vie privée. »

C'est ainsi qu'a été annoncée la première mesure gouvernementale destinée à réglementer sa collecte et son utilisation du NAS. De nombreuses utilisations actuelles seront éliminées d'ici cinq ans et, dorénavant, toutes les nouvelles collectes du NAS proposées pour des raisons administratives, sauf celles qui figurent sur une liste approuvée, devront être autorisées par le Parlement lui-même.

La nouvelle politique défendra les citoyens contre toutes les pressions bureaucratiques naturelles du secteur public et du secteur privé. Pour la première fois, un gouvernement tente de réduire son utilisation de son propre moyen d'identification numérique. Il est plus facile et moins coûteux de reconstituer les œufs d'une omelette (la politique doit coûter 16 millions de dollars, et c'est peut-être une sous-estimation), mais le gouvernement va de l'avant!

Le NAS ne sera plus le principal numéro d'employé du fonctionnaire; il ne sera plus le numéro du service militaire. Les personnes demandant à résider en permanence au Canada n'arriveront plus chez nous avec un NAS, et l'on pourra présenter une demande de citoyenneté sans être obligé d'avoir un NAS. Les pêcheurs commerciaux qui demandent un permis, les contribuables demandant un remboursement de la taxe sur le combustible, les candidats à des bourses et bien d'autres encore seront désormais libérés de la tyrannie du NAS.

Il est paradoxal que le NAS ait pris tant d'importance dans une société comme la nôtre, si férue de liberté. À l'Île-du-Prince-Édouard, on donne aux bébés un NAS comme numéro d'enregistrement de naissance, et certains embaumeurs seraient même allés jusqu'à demander le NAS du défunt. Le cycle est complet, de la naissance à la tombe.

En évitant les abus dans sa propre administration, le gouvernement fédéral a désormais une autorité morale accrue, en plus de son autorité légale, pour faire pression sur les autres paliers de gouvernement et sur le secteur privé. Si l'on continue à exiger la divulgation du NAS sans raison valable, il faudra manifestement adopter une loi restrictive, et ce ne serait que justice.

Un pas en arrière

Trois mois seulement après l'annonce d'une politique extrêmement encourageante de limitation des utilisations du NAS, le Parlement a adopté des modifications à la *Loi de l'impôt sur le revenu*, dont l'une qui oblige les Canadiens à donner leur NAS à leurs institutions financières. Du jour au lendemain, il n'a même plus été possible d'ouvrir un compte bancaire sans donner son NAS. La nouvelle politique a été conçue pour faciliter la communication de renseignements sur les revenus d'intérêts à Revenu Canada; c'est peut-être admirable, mais malheureusement, on n'a à peu près rien fait pour informer le public à l'avance de la raison d'être de cette nouvelle utilisation du NAS.

Le gouvernement avait pourtant promis de consulter le Commissaire à la protection de la vie privée avant de prendre des initiatives dans ce domaine... Il n'en a rien fait avant de présenter son projet de loi. Pour le gouvernement, améliorer l'efficience de la collecte des impôts justifie une nouvelle utilisation du NAS, sans égard, semble-t-il, au danger qu'elle représente pour la vie privée.

La complexité des modifications de la *Loi de l'impôt sur le revenu* est telle que cette nouvelle utilisation du NAS — et les répercussions qu'elle entraîne — ont échappé aux députés et sénateurs, à la presse, voire le Commissariat à la protection de la vie privée. Comment pouvait-on prévoir trouver dans cette Loi une disposition influant sur la protection de la vie privée? On voit à quel point la protection de la vie privée est vulnérable aux assauts les plus inattendus!

Pour la première fois, refuser de donner son NAS est une infraction punissable en vertu de la nouvelle *Loi de l'impôt sur le revenu*. Depuis le début, la loi et les règlements donnent aux institutions gouvernementales le pouvoir d'exiger les NAS, surtout pour des programmes sociaux comme l'assurance-chômage et les pensions. Sans numéro, il n'y a ni assurance, ni prestations. Désormais, à défaut de numéro, il y a une amende de 100 $. (Ceux qui refuseront de payer l'amende écoperont-ils de deux jours de prison?)

C'est une autre première. Jusqu'à l'adoption de ces modifications à la *Loi de l'impôt sur le revenu*, les Canadiens n'étaient legalement tenus de donner leur NAS qu'au gouvernement fédéral. Maintenant, ils sont forcés de le donner aux banques, compagnies de fiducie, maisons de courtage, coopératives de crédit et caisses populaires chaque fois qu'ils font ce qui semble être un investissement portant intérêt. Bravo pour la société de l'ordinateur...

Bien sûr, il faut payer ses impôts. L'application de la nouvelle Loi a été remarquablement conséquente, dès que la déduction de 1 000 $ pour les intérêts a été abolie. Il reste que les implications des nouvelles demandes de NAS — et de la peine imposée à ceux qui refusent de le donner — sont bien plus vastes que quiconque ne semble s'en être rendu compte. Il est vraiment dommage que personne n'ait pensé à se renseigner ou à expliquer la situation.

Si peu de temps après avoir annoncé son admirable politique de restriction de l'utilisation du NAS, le gouvernement autorise des milliers d'institutions du secteur privé (qu'on songe seulement au nombre de succursales bancaires!) à conserver de nouveaux dossiers avec le NAS comme code d'identification. Le fait que l'utilisation abusive du NAS soit frappée d'une amende de 5 000 $ est une piètre consolation.

...et un autre

Dans *Les prochaines étapes*, le gouvernement s'est engagé à élargir le mandat de la Loi aux sociétés d'État fédérales et à leurs filiales. Cette mesure fera presque doubler le nombre d'institutions assujetties à la Loi et, chose plus importante encore, elle fera du gouvernement un véritable chef de file pour le secteur privé. Bref, en mettant en œuvre ces pratiques équitables en matière d'information, le gouvernement mettait de l'ordre dans ses affaires.

Comme de nombreuses sociétés d'État font directement concurrence à des entreprises privées, la décision du gouvernement de les assujettir à la Loi fait vraiment passer le message qu'à son avis, la protection des données peut être un atout, plutôt qu'un obstacle à la bonne conduite des affaires. La Société canadienne des postes doit respecter la Loi depuis cinq ans, et elle a constaté qu'elle pouvait fort bien mener ses affaires en dépit d'une concurrence intense. Il se peut donc fort bien que la grande majorité des sociétés d'État finissent par être assujetties à la Loi (des membres du Commissariat faisant partie d'un groupe de sensibilisation, sont allés rencontrer des représentants de 21 sociétés d'État), mais l'initiative du gouvernement a souffert de la lenteur du processus et surtout de deux omissions de taille. En effet, ni Air Canada, ni Petro-Canada ne figurent sur la liste des institutions qui seront assujetties à la Loi.

Air Canada a été exemptée parce qu'elle n'est plus une société d'État à 100 % : le raisonnement est contestable, puisque le gouvernement continuera d'en être l'actionnaire majoritaire quoi qu'il arrive. Ce fait devrait à lui seul l'obliger à respecter son engagement original. En période de privatisation, ce serait imposer un principe dangereux que d'exempter des sociétés d'État de l'application d'une loi fédérale du seul fait que leur propriété est partagée. Jusqu'à présent, ce motif n'a pas suffi. D'ailleurs, Air Canada est toujours assujettie à la *Loi sur les langues officielles*, et elle le resterait probablement même si elle était complètement privatisée. La protection de la vie privée des clients et des employés d'Air Canada est sûrement aussi importante que celle de leurs droits linguistiques...

D'autres démocraties occidentales ont reconnu la nécessité de protéger par des codes les impressionnantes quantités de renseignements personnels emmagasinées dans les ordinateurs des transporteurs aériens. Si British Airways peut s'accommoder de la législation sur la protection des données du Royaume-Uni, Air Canada devrait pouvoir s'accommoder de la *Loi sur la protection des renseignements personnels*.

Petro-Canada est une société d'État à 100 %, mais sa direction n'a pas voulue être assujettie à la Loi parce qu'elle craint que cela nuise à ses affaires.

Peut-être Petro-Canada aura-t-elle la vie plus facile si elle n'est pas tenue de communiquer à ses clients ou à ses locataires les dossiers de crédit qu'elle détient sur eux, comme elle devrait le faire en vertu de la Loi. Elle aurait d'ailleurs la vie bien plus facile si elle n'était pas obligée de satisfaire aux exigences des droits de la personne ou de la législation sur l'équité en matière d'emploi, mais il n'est pas question de l'en dispenser. La protection du droit à la vie privée des employés et des clients de Petro-Canada est pourtant au moins aussi importante.

Si des institutions aussi en vue qu'Air Canada et Petro-Canada étaient exemptées de la Loi, on pourrait considérer à juste titre que le gouvernement se soustrait à ses propres engagements. En effet, presque toutes les institutions publiques ou privées peuvent imaginer des raisons pour justifier d'être exemptées de lois à caractère réglementaire sur la protection de la vie privée ou sur d'autres principes.

Via Rail pourrait par exemple contester l'application de la Loi, à l'instar de la Société Radio-Canada. Il n'empêche que ces deux sociétés d'État y seront assujetties (bien qu'avec certaines dispositions spéciales de protection des activités journalistiques de la seconde).

Utopisme, ce désir d'assujettir deux sociétés d'État à la Loi quand le secteur privé tout entier, qui comprend des entreprises réglementées par le gouvernement fédéral, échappe totalement à la Loi? Pourquoi s'inquiéter d'Air Canada quand les autres compagnies aériennes canadiennes volent paisiblement sans devoir respecter les contraintes de l'équité en matière d'information? Pourquoi insister pour que les clients de Petro-Canada bénéficient de la protection de la Loi tandis que ceux de leurs concurrents sont livrés à eux-mêmes?

Bien sûr, exempter deux institutions de plus de la Loi — ou au contraire les y assujettir — n'aura pas grand effet sur la qualité globale de la protection de la vie privée au Canada, mais si le gouvernement n'insiste pas pour que ses créatures respectent ses règles, le secteur privé ne l'écoutera pas quand il l'invitera à adopter des codes comme les principes de protection des données de l'Organisation pour la coopération et le développement économiques (OCDE).

Et l'autoréglementation?

Dans ce contexte, les démarches du gouvernement fédéral pour encourager l'entreprise privée à respecter les lignes directrices de l'OCDE que le Canada a signées n'ont guère été efficaces. En

effet, le ministre des Affaires extérieures ne semble pas avoir obtenu de résultats probants lorsqu'il a demandé aux grandes entreprises d'appliquer ces lignes directrices dans leur exploitation.

Le gouvernement fédéral a rencontré à deux reprises les gouvernements provinciaux pour élaborer des stratégies propres à inciter le secteur privé à appliquer les lignes directrices. Toutefois, les parties ne semblent pas s'être entendues sur les secteurs d'activité visés ou sur les stratégies elles-mêmes.

Le gouvernement a besoin d'une approche plus énergique. C'est le strict minimum depuis qu'il a rejeté la recommandation unanime du Comité permanent de la Justice et du Solliciteur général, qui voulait que tout le secteur privé de compétence fédérale soit assujetti à la Loi.

Cette recommandation n'a pas été acceptée (et le Commissaire était d'accord sur ce point), parce que l'autoréglementation semblait alors la méthode optimale : la déréglementation est à la mode. Les quelques expériences d'autoréglementation n'ont pas révélé d'abus endémiques ni même très fréquents. En outre, on peut se demander s'il est possible de concevoir une *Loi sur la protection des renseignements personnels* applicable à toute la gamme des entreprises privées, des banques aux câblodistributeurs. À l'âge du micro-ordinateur, il est inimaginable qu'on puisse appliquer la réglementation de façon parfaitement étanche. D'ailleurs, s'il fallait que le Commissariat soit une gigantesque organisation employant des régiments entiers d'enquêteurs, plus personne ne voudrait en entendre parler.

Par conséquent, pour la plupart des gens, y compris le Commissaire, l'autoréglementation l'emporte sur la réglementation par le gouvernement. Les lois de la deuxième génération sur la protection des données qui ont été récemment adoptées (dans les 12 derniers mois, en Irlande, en Australie et au Japon) se rapprochent bien plus du modèle canadien que des lois de la première génération qui régissaient le secteur privé en Suède et en France. Il reste qu'en l'absence de preuves plus concluantes de l'efficacité de l'autoréglementation, les partisans des codes de protection volontaire des données auront de plus en plus de mal à défendre leur point de vue.

Mais qui décide?

La demande de renseignements personnels poursuit sa croissance exponentielle. Arthur Miller, qui enseigne le droit à Harvard, affirme qu'il ne suffit pas pour voler d'avoir un billet en main quand on se présente à l'aéroport. Pour les transporteurs aériens, les passagers n'existent pas à moins que le code numérique voulu apparaisse à l'écran d'affichage; ils ne sont qu'une version tridimensionnelle de l'information affichée. Et M. Miller de poursuivre :

> « Ce n'est pas simplement un système de réservation de billets d'avion. L'ordinateur a mon nom, mon numéro de téléphone, le numéro de ma carte de crédit et le nom des gens avec qui je prends l'avion. Il sait si j'ai fait réserver une chambre d'hôtel ou loué une voiture par son intermédiaire. C'est un véritable dossier. »

Il y a bien d'autres dossiers : pas moyen de dormir dans un lit Sheraton à moins d'être reconnu par l'ordinateur. Nous finissons par nous rendre compte que notre vie est contrôlée par une banque de données après l'autre, au gré des ordinateurs.

C'est le prix de la commodité et de l'efficience, et personne n'irait proposer qu'on détruise les ordinateurs. Néanmoins, il faudrait qu'on adopte et qu'on respecte des règles fondamentales de traitement des énormes quantités de renseignements personnels collectés par tout un chacun. Le danger, c'est que les collections de données peuvent servir, sur simple pression d'un bouton, à prendre des décisions cruciales pour nous. Arthur Miller le dit bien :

> « Nous avons fini par comprendre qu'il est impossible de souscrire une assurance, d'obtenir du crédit, de décrocher certains emplois ou d'avoir accès à certains avantages gouvernementaux sans faire approuver nos dossiers; nous savons que des gens passent nos dossiers au peigne fin. Nous ne savons pas qui sont ces gens, ni où ils sont. Nous ne savons pas non plus quels sont les critères décisionnels. »

Ce que nous savons — et si nous ne le savons pas, nous devrions le savoir! — c'est que les renseignements en mémoire sur nous peuvent être erronés. Et pourtant, s'il n'existe pas de législation sur la protection des renseignements personnels ou de codes efficaces de respect volontaire de ces renseignements, nous n'avons aucun moyen d'accès à nos dossiers pour les corriger. Sans loi ou sans code, rien ne peut empêcher l'expansion tentaculaire de l'industrie de la vente et de l'échange de renseignements personnels informatisés et de données sur les habitudes des consommateurs (établies par l'examen de leurs achats par carte de crédit et par commandes postales) et sur leurs dons à des œuvres de charité ou à des organismes politiques.

Qui décide? Sommes-nous maîtres des renseignements personnels qui nous concernent? Devons-nous céder le pas aux collecteurs et aux marchands de renseignements personnels, armés de leurs merveilleuses machines? En devenant des « objets de données », nous ne devrions pas perdre la moindre parcelle de notre humanité. Autrement, nous serions les esclaves de nos machines, et les sociétés de l'information seraient devenues des « sociétés surveillées », réalisant ainsi la sombre prophétie du professeur David Flaherty, de l'Université Western.

Le professeur Flaherty, un spécialiste de réputation internationale de la législation sur la protection de la vie privée et des données, s'est exprimé en termes quasi apocalyptiques :

« Les bases de données informatisées d'aujourd'hui rendent possible un contrôle relativement intégré des citoyens des pays occidentaux. C'est la prolifération de ces fichiers d'information publics et privés, plutôt que l'existence de l'un ou l'autre d'entre eux, qui est le véritable défi pour les protecteurs de la vie privée. Nous devons absolument penser aux implications de pratiques de surveillance comme celle-là pour la protection des droits de la personne. En Amérique du Nord, l'application de la technologie de l'information progresse à un rythme de loin plus rapide que l'évolution de la réglementation et des mesures de contrôle. »

Être privé de son pouvoir de contrôler ce que le monde sait de soi est humiliant et déshumanisant. Ceux qui réclament leur droit à la vie privée n'ont rien du marginal ou du dilettante. Ils vont au cœur même de l'intégrité et de la dignité de l'être humain et du genre de société que nous souhaitons tous. C'est là que la protection de la vie privée prend toute son importance.

Et la protection de la vie privée est particulièrement critique dans les relations entre les citoyens et leurs gouvernements, étant donné que l'État a d'énormes pouvoirs d'extraction et d'utilisation des renseignements personnels.

Pourtant, la conclusion d'un concordat pour la protection de la vie privée dans le monde de l'entreprise est en passe de devenir presque aussi indispensable. En effet, même quand nous donnons volontairement des renseignements personnels (et ce n'est souvent pas le cas, par exemple pour une demande de crédit), des règles claires s'imposent si nous voulons que l'individu conserve au moins un certain contrôle sur les utilisations qu'on en fera.

Certains spécialistes du domaine, dont le professeur Flaherty, ont fini par conclure qu'il est désormais trop tard pour qu'on puisse aboutir à un concordat sur la protection des renseignements personnels dans le secteur privé. Selon eux, seule la Loi peut faire obstacle aux puissantes technologies nouvelles et donner à la vie privée un minimum de protection. Bref, il faut revenir aux régiments d'enquêteurs et aux bureaucraties monumentales.

Un autre spécialiste de la protection de la vie privée, le professeur James Rule, de l'Université de l'État de New York, déclarait récemment que le meilleur moyen d'assurer la protection des renseignements personnels consisterait à donner à chacun un « droit d'auteur » sur l'utilisation commerciale de l'information personnelle le concernant. Cette information ne pourrait ni être vendue, ni donnée en contrepartie d'un avantage quelconque sans l'autorisation de l'intéressé. C'est un concept ingénieux et fascinant, voire logique, mais il est bien peu réaliste, et manifestement impossible à appliquer.

Ce sont là des solutions de désespoir inspirées par des visions cauchemardesques. Il y a sûrement un moyen terme. Les règles de respect volontaire de la vie privée, telles que les lignes directrices de l'OCDE, sont parfaitement logiques et, pour peu qu'on les applique, elles semblent promettre des garanties raisonnables. Néanmoins, le moment est venu pour le gouvernement d'imposer dans ce domaine un régime de volontariat analogue à celui de l'armée.

Les entreprises réglementées par le gouvernement fédéral, qui auraient dû être assujetties à la Loi d'après la recommandation unanime du Comité du Parlement, devraient être le point de départ de cette démarche. En plus de poursuivre avec une énergie accrue une stratégie de coopération avec les provinces afin d'encourager le respect volontaire des lignes directrices de l'OCDE, le gouvernement du Canada devrait s'attaquer au secteur privé qu'il réglemente, en ouvrant un second front pour la protection des renseignements personnels. Il devrait enjoindre au secteur privé de se donner des codes de protection de la vie privée efficaces, dans un délai précis, puis d'en informer clients et employés (qui seront ravis!) sous peine de se voir imposer une loi exécutoire.

Les partisans d'une loi sur la protection des renseignements personnels dans le secteur privé ont raison sur un point : les invitations aimables n'ont pas eu grand effet. Il reste qu'il est préférable d'augmenter un peu la pression plutôt que d'échafauder un lourd appareil de protection législative de la vie privée.

Vous voulez des données? Composez Bell!

Le Commissaire ne s'est pas contenté d'être un simple spectateur et d'évaluer la prestation du gouvernement. Il s'est lancé dans la partie, lorsqu'il a appris en novembre dernier que le Conseil de la radiotélévision et des télécommunications canadiennes se demandait s'il fallait autoriser Bell Canada à vendre la base de données des abonnés aux pages blanches et aux pages jaunes de son annuaire téléphonique, sous forme lisible à la machine. Le Conseil se demandait à qui et sous quelles conditions Bell aurait pu le faire. La demande n'émanait pas de la compagnie de téléphone, mais bien d'entreprises qui convoitaient sa base de données. Quel bel exemple de l'intensité des pressions exercées en vue d'échanges à grande échelle de renseignements personnels informatisés! (C'est aussi un bon exemple de la façon dont un organisme de réglementation intelligent devrait être conscient des enjeux.)

Avec une remarquable retenue, le CRTC a déclaré que le fait de communiquer ces renseignements sous forme lisible à la machine risquait d'accroître les inquiétudes quant à la protection des renseignements personnels sur les consommateurs. Il s'agit bien d'accroître les inquiétudes! Même s'il n'y a rien de plus public qu'un annuaire téléphonique, les clients de Bell ont de bonnes raisons de s'inquiéter. Le Commissaire les a exposées dans une intervention officielle, en demandant au CRTC de ne pas obliger Bell Canada à offrir la base de données de ses annuaires à tous les acheteurs éventuels.

Le Commissaire est intervenu parce que la qualité des données se modifie lorsque les noms, les adresses et les numéros de téléphone sont transférés d'un support papier à des disques de traitement électronique des données. La vie privée des consommateurs est particulièrement menacée en raison de l'accessibilité, de la transférabilité et de la transformabilité infiniment accrues (les mots mêmes sont menaçants) des données lisibles à la machine. Et rien ne nous touche de plus près qu'un annuaire téléphonique.

Une entreprise a déjà transféré sur un disque au laser de 4,7 pouces les noms, adresses et numéros de téléphone de 7,9 millions des 8,5 millions de ménages canadiens. Le processus a été long et coûteux (au-delà de 1 million de dollars, et encore au Pakistan).

Ce n'était qu'un début. Le même disque au laser contient maintenant les coordonnées de chaque ménage, à un mètre près, sur une carte topographique du Canada, avec les noms des voisins, la circonscription électorale et la période d'occupation à l'adresse indiquée, en plus de 12 champs démographiques (vendus globalement par Statistique Canada), notamment sur le revenu, la langue officielle, la religion et le nombre d'enfants. Toute cette information fait partie du domaine public, mais dès qu'on y ajoute des renseignements sur les cartes de crédit ou sur les comptes bancaires, à supposer qu'on puisse les obtenir par des moyens honnêtes ou pas, on aboutit à un profil de la population à échelle aussi grande que systématique.

C'est un outil de rêve pour la commercialisation, mais un cauchemar pour la protection de la vie privée. L'information lisible à la machine peut être manipulée de toutes les façons imaginables pour le démarchage téléphonique ou postal. Et pourtant, cette utilisation-là serait virtuellement innocente. Les inscriptions du genre sont aussi un moyen de contrôle ou de suivi non seulement pour les spécialistes de la commercialisation, mais aussi pour les criminels et pour les organismes policiers.

Les abonnés du téléphone n'ont jamais imaginé, encore moins consenti à, une telle intrusion dans leur vie privée lorsque leur nom paraît dans le bottin téléphonique. Malheureusement, avec la technologie moderne, le danger est réel et imminent.

La protection de la vie privée dans le contexte du SIDA

Sur un autre front, comme il l'avait promis dans son rapport de l'année dernière, le Commissaire a préparé des recommandations pour s'assurer que les renseignements personnels sur le SIDA seront traités par le gouvernement fédéral conformément à l'esprit et à la lettre de la Loi. Dans son rapport, intitulé *Le SIDA et la Loi sur la protection des renseignements personnels*, le Commissaire confirme que la réaction d'envergure nationale qui s'impose dans le cas du SIDA est peut-être la question de protection de la vie privée la plus délicate et la plus émotive de notre époque. Dans son rapport, le Commissaire recherche un équilibre fugace entre la protection de l'intimité de ceux qui souffrent du SIDA ou qui sont porteurs du VIH (le virus qui cause le SIDA) et la divulgation nécessaire à la protection de leur entourage.

Par compassion pour les porteurs du virus, il faut les protéger contre le traumatisme qu'entraînerait une intrusion inutile dans leur vie privée et une divulgation de leur état. Apprendre qu'on est victime du SIDA continue d'être un arrêt de mort. En fait, d'après certains, être porteur du VIH, c'est la mort prochaine.

Les réactions illogiques et extrémistes du public et des gouvernements à l'annonce que quelqu'un souffre du SIDA ou qu'il est porteur du VIH peuvent parfois modifier de façon très réelle les conditions de l'appartenance d'une personne à la société, en limitant son accès à l'école, au travail, aux soins médicaux, voire à sa famille et à ses amis. En faut-il davantage pour réclamer le plus de respect possible pour la vie privée des victimes?

D'un autre côté, la divulgation s'impose, même si elle n'est pas nécessaire aussi souvent qu'on le dit parfois. Les scientifiques et les médecins ont peut-être besoin de savoir qui sont les victimes du SIDA et les porteurs du VIH, dans leur recherche des moyens de ralentir, de stopper ou de traiter la maladie. Ces préoccupations contradictoires nécessitent souvent des mesures conflictuelles.

Le Commissaire conclut dans son rapport que la vérification obligatoire des anticorps du VIH pour des groupes comme les fonctionnaires, les détenus des pénitenciers fédéraux, les immigrants et les visiteurs à long terme au Canada enfreindrait la Loi. En effet, celle-ci interdit la collecte de renseignements personnels qui ne sont pas liés directement à un programme ou une activité ressortissant au mandat législatif d'une institution gouvernementale. Il se fait qu'une vérification pareille n'est pas un élément fondamental d'un programme législatif actuel.

Bien sûr, le Parlement peut prévaloir sur la Loi et donner au gouvernement le pouvoir d'obliger certains groupes à subir volontairement des examens de dépistage des anticorps du VIH. Toutefois, les mesures de ce genre seraient une réaction hystérique exagérée à la prolifération du SIDA, du moins dans l'état des connaissances actuelles de la maladie.

Les avantages pour la santé publique susceptibles de résulter d'une vérification à si grande échelle sont pour le moins douteux; les effets dévastateurs de sa corollaire, l'intrusion dans la vie privée des gens, l'emporteraient de

loin. Heureusement, les partisans de la protection des renseignements personnels sont d'accord à ce sujet avec les plus éclairés des médecins : il faudrait toujours que les gens se soumettent à des examens de dépistage du SIDA de leur plein gré, en bénéficiant de conseils avant et après les examens.

Le gouvernement du Canada a un rôle important à jouer pour faire en sorte que le SIDA soit traité avec sensibilité dans les milieux de travail. Le rapport du Commissaire invite instamment le Conseil du Trésor, en sa qualité de plus important employeur au Canada, à formuler une politique exhaustive sur le SIDA dans les milieux de travail.

Le caractère confidentiel des renseignements personnels est partie intégrante de la politique du milieu de travail proposée par l'Organisation mondiale de la santé. L'employé ne devrait pas être forcé de dire à l'employeur s'il est porteur ou pas du VIH, et il n'est pas nécessaire non plus qu'il le dise à ses collègues. Si l'employé communique de son plein gré des renseignements personnels liés au SIDA, il faudrait leur accorder une excellente protection et, avant son embauche, le futur employé ne devrait être soumis à aucun examen direct ou indirect (évaluation des comportements à risques ou questions au sujet des examens préalables) de dépistage du VIH.

L'une des raisons que les gens donnent le plus souvent lorsqu'ils hésitent à subir volontairement des examens de dépistage des anticorps du VIH, c'est qu'ils craignent de ne pas pouvoir contrôler la mesure dans laquelle des tiers auront accès à cette information.

La Loi elle-même précise 13 cas dans lesquels les ministères peuvent communiquer des renseignements personnels à des tiers sans le consentement des intéressés. Compte tenu de la nature particulièrement délicate des renseignements liés au SIDA, *Le SIDA et la Loi sur la protection des renseignements personnels* recommande qu'on applique une procédure très rigide avant de divulguer des renseignements de ce genre.

Chose plus importante encore, la décision de divulguer quoi que ce soit du genre à des tiers devrait toujours être prise par le responsable de l'institution gouvernementale, en fonction des éléments suivants :

1. les raisons rendant la divulgation nécessaire;

2. le préjudice que cette divulgation pourrait entraîner pour la ou les personnes intéressées;

3. la capacité du requérant de garder le secret et

4. la capacité du requérant d'utiliser les renseignements exclusivement aux fins pour lesquelles ils avaient été demandés initialement.

Dans tous les cas, il devrait incomber au requérant de justifier la communication des renseignements sans le consentement de la ou des personnes intéressées.

Ces recommandations ont été conçues de façon à refléter un compromis convenable entre la nécessité de la protection des renseignements personnels et les besoins légitimes de certaines institutions gouvernementales. Si la compréhension que le public a du SIDA et de sa transmission change — et s'il change aussi d'attitude — les recommandations pourraient être remises en question, tout comme si l'on découvrait un vaccin ou une cure. Le rapport ne l'a pas caché :

> « Cette terrible maladie a spontanément fait surgir dans l'humanité l'espoir que soit rapidement découvert un remède ou un vaccin efficace. Mais l'espoir n'allège en rien les responsabilités que doit maintenant assumer la société. Les principes énoncés dans le présent document dans le but de répondre aux problèmes que suscite, sur le plan de la protection de la vie privée, le traitement des renseignements personnels concernant les personnes séropositives et sidatiques n'apporteront peut-être guère de réconfort à long terme, mais au moins, ils ont le mérite d'humaniser la réaction de la société. Pour le moment, peut-être ne pouvons-nous rien faire de mieux. »

À l'aube de l'ère biotechnologique

Dans l'ensemble, le gouvernement obtient son information sur les citoyens par des méthodes traditionnelles : des enquêtes, des formulaires, des lettres, voire l'observation directe. Pourtant, il est possible d'abuser même de ces méthodes, au point de porter gravement atteinte à la vie privée. Toutefois, il y a plus grave : les techniques de collecte « intrusives » se répandent de plus en plus.

Ces techniques, dont certaines sont très récentes, permettent de tirer des renseignements sur les gens directement de leur organisme. C'est le cas de l'alcootest et du polygraphe. Les analyses d'urine et de sang et le codage génétique sont en train de s'imposer comme moyens de révéler des secrets personnels ignorés parfois même des premiers intéressés.

Les milieux policiers sont passés maîtres dans l'utilisation de ces méthodes, qui sont toutefois de plus en plus souvent utilisées comme techniques d'évaluation hors du contexte pénal. Seriez-vous un employé loyal et digne de confiance? Risquez-vous d'avoir des comportements dangereux pour autrui? Avez-vous enfreint les règles régissant une activité qui vous intéresse? Êtes-vous génétiquement prédisposé à certaines maladies, ou vulnérable à certains styles de personnalité? Les employeurs du secteur public et du secteur privé sont tentés d'avoir recours à la biochimie pour répondre à ces questions.

Ainsi, le ministère de la Défense nationale fait des analyses de sang des employés désireux de suivre des cours sur la défense aux États-Unis, afin de vérifier s'ils sont porteurs du VIH. Le SCRS se sert d'un polygraphe pour vérifier si les candidats à des postes dans son organisation sont loyaux et dignes de confiance. Enfin, Transports Canada s'interroge sur l'opportunité de soumettre les travailleurs des transports à des analyses d'urine pour voir s'ils consomment des drogues illégales.

Sports Canada fait des pressions pour que les athlètes qu'il subventionne subissent des analyses d'urine pour y détecter la présence de substances interdites (mais pas nécessairement illégales) capables d'améliorer les performances des athlètes, et donc de leur donner un avantage injuste. La GRC se sert de matériaux génétiques à des fins d'identification, et elle doit mettre sur pied un répertoire national d'identification génétique analogue à celui des empreintes digitales qu'elle conserve déjà. En outre, les chercheurs poursuivent leurs travaux en vue de l'établissement de profils physiques et comportementaux des individus grâce à des analyses de l'ADN.

À en croire un commentateur, nous passerions de l'ère de l'information à l'ère biotechnologique. La transition exposera la protection de notre vie privée à des risques comme nous n'en avons jamais courus.

Pour que la protection de la vie privée ait un sens dans les années 1990 et au-delà, il nous faudra prendre grand soin de veiller à ce qu'on impose des contrôles efficaces contre les méthodes nouvelles — et plus intrusives que jamais — de collecte de l'information. Pourtant, les années 1980 tirent à leur fin, et il semble bien que nos dirigeants ne penchent pas dans ce sens-là.

Certains hauts fonctionnaires et autres personnes influentes qui ont témoigné à l'Enquête Dubin se sont dits très favorables à l'idée d'obliger les athlètes subventionnés par le gouvernement fédéral à subir des analyses d'urine aléatoires à l'improviste. Il y a bien sûr de bons arguments pour justifier une mesure pareille, mais ce qui est inquiétant, c'est qu'une politique gouvernementale, même dans un secteur précis et avec le consentement tacite des athlètes, semble faire fi d'une notion fondamentale pour la vie privée de chacun, à savoir la présomption d'innocence. La nécessité d'empêcher une intrusion dans la vie privée des gens à moins qu'on puisse raisonnablement soupçonner un méfait précis a été clairement établie par la Cour suprême, dans le contexte de la Charte canadienne des droits et libertés. Le principe a toujours été maintenu, sauf dans des cas d'exception, pour protéger la vie humaine, par exemple en utilisant l'alcootest à l'improviste le long des routes.

Néanmoins, dans le cas des athlètes, la fierté nationale offensée semble largement suffire à justifier le rejet d'un principe fondamental de la liberté. Si nous pouvons accepter les intrusions nécessaires dans le cas des athlètes, et peut-être le juge Dubin conclura-t-il que nous le pouvons, ne sera-t-il pas plus facile pour les employeurs de justifier leurs intrusions biologiques chez leurs employés actuels ou éventuels? L'enquête sur l'utilisation des drogues par les athlètes risque d'avoir sur notre philosophie de la protection de la vie privée des retombées qui déborderont les stades, et plus encore les vestiaires.

Si le Commissaire souligne dans ses rapports annuels son inquiétude à l'égard du couplage informatique, autrement dit de la comparaison de bases de données différentes afin d'en tirer des profils de certaines personnes, c'est que la méthode équivaut à une perquisition et à une saisie de dossiers sans motifs raisonnables. C'est précisément pour la même raison qu'il continuera à suivre de près l'évolution des programmes d'analyse biotechnologique, afin de protéger la vie privée des innocents.

Sécurité informatique

« La sécurité consiste à protéger l'ordinateur de l'intervention humaine; la protection de la vie privée, c'est l'inverse. »

Robert P. Bigelow, dans *Computer Law and Security Report*, mars-avril 1989

Ce serait bien trop simple! Dans les bureaux hautement automatisés, la sécurité informatique est essentielle pour protéger le personnel des autres, et c'est peut-être le but ultime des défenseurs de la vie privée.

Dans le monde décentralisé du traitement des données que nous connaissons, un système informatique absolument sûr est un idéal impossible. Aujourd'hui, les spécialistes de la sécurité informatique parlent de systèmes « fiables » plutôt que « sûrs ». (Belle réflexion sur notre société, ce mot « fiable » qui véhicule une certaine méfiance!)

Les systèmes d'information de gestion (SIG) sortent à peine de l'adolescence et, depuis le milieu de la dernière décennie, l'ordinateur est devenu partie intégrante de l'administration gouvernementale, grâce à ses nombreux talents : il est capable de traitement multiple, de manipulation de fichiers énormes, de transmission de données sur de grandes distances en quelques secondes et d'ouverture des ressources d'information à de nombreux utilisateurs.

De nos jours, il n'est plus rare de trouver dans un bureau gouvernemental des postes de travail polyvalents reliés à un ordinateur central ou à un réseau d'ordinateurs, en partageant consciemment ou inconsciemment les données, voire dans certains cas les logiciels.

Au cours de la dernière année, le Commissariat s'est intéressé au labyrinthe de la sécurité informatique, cet univers déroutant qui a une terminologie et une technologie bien à lui. La panoplie des ennemis internes des systèmes informatiques est étrange : saucissons, pièges, « bombes » à retardement, chevaux de Troie et vers, tout y est. Les armes de ceux qui s'attaquent aux ordinateurs de l'extérieur sont tout aussi exotiques; ce sont des virus, des perturbations préméditées, des commutations et des explorations illicites, des croisements de réseaux et des décodages frauduleux.

Ceux qui cherchent la parade sont aussi « colorés ». Aux États-Unis, le ministère de la Défense publie ses normes de sécurité dans le « Livre orange » et les explique dans le « Livre jaune ». La sécurité des systèmes d'établissement de réseaux fait l'objet du « Livre framboise », et ainsi de suite.

Le monde du SIG pose d'énormes problèmes de sécurité face auxquels le Commissariat commence à peine à acquérir la compétence nécessaire pour définir les difficultés et pour proposer des solutions logiques et pratiques. Au cours de l'année à venir, il insistera particulièrement sur la sécurité des systèmes de TED, dans ses vérifications régulières des institutions gouvernementales.

Il faut souligner tout particulièrement la valeur du travail du Centre de sécurité des systèmes du Centre de la sécurité des télécommunications, créé en août 1988 pour accroître la compétence en sécurité informatique de la GRC et du MDN et pour offrir au gouvernement du Canada de nouvelles possibilités d'évaluation des produits de sécurité pour les ordinateurs et les réseaux. La *Loi sur la protection des renseignements personnels* est l'un des éléments qui incite le Canada à se donner ses propres critères d'évaluation de la sécurité informatique. En effet, le gouvernement reconnaît que, même si c'est la protection des renseignements touchant la sécurité nationale qui pose les difficultés techniques les plus ardues, les problèmes les plus fréquents sont liés à la nécessité de protéger les renseignements personnels détenus par le gouvernement.

Le Commissaire est heureux de cette initiative, et c'est avec plaisir qu'il envisage un échange durable d'information et d'idées avec le Centre de sécurité des systèmes.

Les dossiers du SCRS

Une autre collection de renseignements personnels très délicats a continué de préoccuper le Commissaire depuis l'an dernier : il s'agit des dossiers dont le Service canadien du renseignement de sécurité (SCRS) a hérité de l'ancien Service de sécurité de la GRC. Depuis que la définition des « menaces envers la sécurité du Canada » a été précisée, une grande partie de l'information contenue dans ces dossiers ne répond pas aux critères de collecte prévus par la *Loi sur le Service canadien du renseignement de sécurité*, du moins d'après le comité de surveillance des activités de renseignement de sécurité.

Bref, le SCRS se trouve par conséquent dans une situation fausse, étant donné qu'il est le gardien de renseignements personnels qu'il n'aurait pas le droit de recueillir en vertu de son mandat actuel.

La solution paraît bien simple : il suffit de retirer les vieux dossiers!

Le SCRS a créé un service qu'il a chargé d'étudier les dossiers, d'en tirer les renseignements qui continuent de présenter de l'intérêt pour lui et d'éliminer le reste. Malheureusement, le procédé est très lent; en outre, certains des dossiers ont été « séquestrés », tandis que d'autres ont fait l'objet de règles spéciales régissant l'accès interne aux dossiers et leur utilisation par le personnel. Le SCRS et les Archives nationales se sont lancés dans des consultations afin de déterminer les renseignements à archiver et les conditions applicables en pareil cas.

Les déchiqueteuses ont pourtant bien servi! Depuis la levée du moratoire sur la destruction des dossiers qui avait été imposé en 1985, après l'intervention de la Commission Deschênes sur les criminels de guerre, on a retiré environ 120 000 dossiers du Service de sécurité, dont 67 000 que la GRC avait déjà prévu de détruire, et 53 000 que le SCRS a examinés avant de décider de les retirer. Il est réconfortant de constater qu'après examen, le SCRS a conservé moins de 100 dossiers. Cela dit, des milliers et des milliers de dossiers ne passeront pas par les déchiqueteuses avant des années.

En outre, les vieux dossiers de la GRC ont créé d'autres problèmes au SCRS. Comme il y est autorisé en vertu de la *Loi sur la protection des renseignements personnels*, celui-ci s'abstient de confirmer ou de nier l'existence de renseignements ayant conservé leur utilité pour lui. Les renseignements de ce genre sont conservés dans le fichier SRS/P-PU-010. Le SCRS ne veut pas non plus confirmer ou nier le fait qu'il n'existe pas de renseignements quand un requérant présente une demande d'accès à ce fichier en vertu de la *Loi sur la protection des renseignements personnels*. Le Commissaire et la Cour fédérale ont reconnu que ce qu'on appelle « l'effet de mosaïque » oblige le SCRS à adopter cette approche.

Néanmoins, le SCRS confirme l'existence de certains renseignements personnels recueillis par l'ancien Service de sécurité de la GRC. Les vieux renseignements de ce type, qui ont perdu leur caractère délicat, sont conservés dans le fichier SRS/P-PU-015. Leur existence est confirmée, et ils sont communiqués aux requérants sous réserve des exemptions expresses précisées dans la *Loi sur la protection des renseignements personnels*. Il n'a pas été possible au Commissaire de s'entendre avec le SCRS sur des lignes directrices définissant les renseignements « moins critiques », en dépit de la bonne volonté manifeste dont le SCRS a fait preuve en réponse aux préoccupations soulevées par le Commissaire dans son dernier rapport annuel.

Pour chaque demande d'accès reçue, le SCRS décide à quel fichier (010 ou 015) verser les renseignements recueillis par l'ancien Service de sécurité de la GRC. Il semble que ce soit la seule façon pratique de procéder jusqu'à ce que tous les dossiers qui ne répondent pas aux critères de collecte de la *Loi sur le Service canadien du renseignement de sécurité* aient été retirés.

Le Commissaire est heureux de pouvoir déclarer que le SCRS compte accélérer son examen et son retrait des vieux dossiers. Au cours des deux prochaines années, il devrait en avoir examiné et retiré deux fois plus qu'il ne l'a fait depuis cinq ans. Le Commissaire applaudit à cette initiative, mais il estime que le procédé devrait être suivi par un observateur indépendant, pour que toute l'information qui n'est pas « strictement nécessaire », aux termes de l'article 12 de la *Loi sur le Service canadien de renseignements de sécurité*, soit bel et bien retirée plutôt que simplement recyclée sous une autre forme.

L'Inspecteur général (en vertu des articles 30 et 31 de la *Loi sur le Service canadien du renseignement de sécurité*), le comité de surveillance des activités de renseignement de sécurité (en vertu de l'article 40 de ladite loi) et le Commissaire (en vertu de l'article 37 de la *Loi sur la protection des renseignements personnels*) semblent tous avoir le pouvoir et la responsabilité nécessaires pour assurer cette inspection indépendante.

Au cours des prochains mois, le Commissaire consultera les parties intéressées afin de déterminer les moyens d'assurer ce suivi du retrait des dossiers en évitant les dédoublements d'efforts.

Qu'est-ce qu'il y a avec le chèque?

Les listes de distribution postale : tout le monde comprend leurs implications pour la protection des renseignements personnels dans le secteur privé. Cela dit, bien peu d'organismes publics ou d'entreprises privées ont des listes de distribution aussi importantes et aussi à jour que le gouvernement fédéral.

Songeons aux trois listes suivantes, par exemple :

— la liste des employés du gouvernement (y compris les membres des Forces armées et de la GRC), c'est-à-dire 350 000 personnes;

— la liste des prestataires des allocations familiales, des pensions de vieillesse et du Régime de pensions du Canada, soit environ 5,5 millions de noms et d'adresses;

— la liste de l'impôt sur le revenu (environ 17 millions de personnes).

Ces trois listes seraient une véritable mine d'or pour les expéditeurs postaux. D'ailleurs, certains les ont déjà demandées sans vergogne.

Ainsi, une maison de publication a demandé à Santé et Bien-être social Canada de lui fournir la liste de tous les prestataires du Régime de pensions du Canada et de toutes les personnes désireuses d'y adhérer. Elle voulait leur envoyer une brochure publicitaire offrant des services juridiques à tous ceux qui éprouvent des difficultés à cet égard.

Le gouvernement fédéral n'a pas le droit de vendre ou de donner ses listes de distribution, mais encore faut-il voir comment il les utilise lui-même... Les ministères et organismes fédéraux savent très bien qu'avec les enveloppes de leurs chèques, ils ont un moyen économique de communiquer avec leur clientèle. Le coût d'un ajout dans ces enveloppes est infime par rapport à celui d'une campagne de publicité, et le public ciblé est atteint avec une efficacité inégalée. En fait, ce serait un excellent moyen de vanter les bienfaits de la *Loi sur la protection des renseignements personnels*! (« Savez-vous à quelle protection vous avez droit pour votre vie privée? »)

Les prestataires des allocations familiales et des pensions ont l'habitude de trouver des avis dans l'enveloppe de leur chèque mensuel. Est-ce une atteinte à leur vie privée?

Pas du tout, à condition que les renseignements communiqués soient directement liés au mandat du ministère au nom duquel le chèque est émis. Ainsi, Santé et Bien-être social Canada peut fort bien informer les retraités d'un changement de leurs prestations ou rappeler aux parents de faire vacciner leurs enfants en temps voulu.

Les risques d'abus sont néanmoins omniprésents. Le Conseil du Trésor s'en est rendu compte, tout à son honneur. Il oblige donc les ministères à obtenir son autorisation pour mettre des avis quelconques dans leurs envois ordinaires. La fiche de route de l'administration fédérale est généralement bonne, mais en dépit d'un suivi plus serré que jamais, 5 des 50 envois de l'an dernier n'avaient rien à voir avec la raison d'être initiale de la liste de distribution en cause.

Par exemple, le gouvernement a envoyé dans une enveloppe adressée aux 9 millions de prestataires des allocations familiales, des pensions de vieillesse et du Régime de pensions du Canada de l'information sur l'Accord de libre-échange canado-américain. En outre, il a envoyé et il envoie encore aux fonctionnaires des chèques de paye accompagnés d'annonces les invitant à acheter des obligations d'épargne du Canada et à contribuer à Centraide. Manifestement, il y a là des risques de conflit. Dans sa politique de communication très logique, le gouvernement enjoint aux ministères et aux organismes d'informer le public de leurs activités. Les obligations d'épargne du Canada sont essentielles au financement des activités gouvernementales, et les personnes désireuses d'en acheter aiment manifestement être informées de l'émission des obligations et de la méthode de retenue automatique des paiements. De même, Centraide est largement tributaire des contributions des fonctionnaires, qui sont grandement facilitées par le système de retenue à la source.

Le principe posé par la Loi est pourtant clair : les renseignements recueillis pour une raison donnée ne peuvent pas l'être pour une autre.

Il y aura dans ce contexte des cas d'application de la Loi difficiles, pour lesquels il faudra beaucoup de jugement. Le Commissaire ne tient pas du tout à empêcher Centraide d'accomplir sa noble mission. Par contre, il tient beaucoup à empêcher le gouvernement de se servir de ses envois pour faire de la politique. Qu'il émane du gouvernement ou pas, le courrier indésirable est toujours indésirable.

Il faut donc surveiller de près tout ce qui accompagne les chèques du gouvernement.

Le Commissaire a entrepris des pourparlers avec le Conseil du Trésor en vue de l'établissement de lignes directrices grâce auxquelles les envois généraux du gouvernement respecteront la Loi.

Direction générale des plaintes

L'étonnante augmentation de 20 p. 100 du nombre des plaintes déposées en 1988–1989 (1050, comparativement à 691 l'année précédente) est difficile à expliquer. Peut-être reflète-t-elle simplement un retour à la tendance établie depuis le début, à savoir une augmentation annuelle de 10 p. 100, ce qui ferait de la baisse de 1987–1988 une aberration largement compensée cette année par l'augmentation massive de la charge de travail. Quoi qu'il en soit, rien ne laisse entendre qu'il faut imputer l'augmentation à une résistance croissante à l'esprit ou à la lettre de la Loi.

L'augmentation globale du nombre de plaintes se double d'une prolifération des plaintes portant sur la lenteur avec laquelle les ministères et organismes répondent aux demandes. C'est décevant, car le Commissaire avait espéré que le problème des retards s'éliminerait de lui-même à mesure que les institutions prendraient de l'expérience. En fait, le Commissariat a enquêté sur près de 400 plaintes au sujet de retards, dont 250 contre le Service correctionnel du Canada, en raison de l'augmentation marquée du nombre de demandes adressées à cet organisme.

Néanmoins, malgré l'augmentation substantielle du nombre de plaintes reçues pendant l'année, le Commissaire et ses collaborateurs se sont efforcés de régler les 296 affaires reportées de l'an dernier. À la fin de l'exercice, il n'en restait plus que quatre en souffrance.

Les enquêteurs ont fermé 1028 dossiers pendant l'année, ce qui représente une augmentation de 56 p. 100 par rapport à 1987–1988. La Direction générale continue à réduire la période d'enquête. La nouvelle norme est d'en moyenne trois mois et d'au plus six mois. À la fin de 1988–1989, 94 p. 100 des dossiers de plaintes étaient actifs depuis moins de six mois.

Cette accélération s'explique partiellement du fait que la Direction générale compte trois nouveaux postes d'agents, obtenus en prévision du moment où les sociétés d'État seront assujetties à la Loi. À la fin de l'année, ce n'était pas encore fait, de sorte que les nouveaux enquêteurs ont pu aider le Commissariat à absorber le flot de nouvelles plaintes. Comme l'effectif de la Direction générale est désormais complet, le Commissariat a confiance qu'il pourra continuer à respecter les nouvelles normes, au moins jusqu'à ce que les sociétés d'État entrent dans la danse.

Question de statistiques... les noms changent, les notions restent

La terminologie utilisée pour décrire le règlement des plaintes a été modifiée par rapport à celle des années précédentes, afin que les ministères et organismes puissent utiliser une terminologie uniforme dans leurs rapports statistiques au Conseil du Trésor et au Commissariat. Après des discussions avec le Conseil du Trésor et toutes les autres parties, la terminologie suivante a été établie :

Non fondée (auparavant « rejetée »)

Bien fondée — résolue (auparavant « justifiée »). Après négociation, le Commissaire est arrivé à ce qu'il considère comme une solution raisonnable. Cela ne signifie pas toujours que le plaignant est entièrement satisfait.

Bien fondée. Il y a eu infraction de la Loi, et il n'a pas été possible d'y remédier, soit parce que les documents étaient introuvables ou déjà détruits, soit parce que le délai était dépassé. On dit aussi qu'une plainte est bien fondée quand le requérant s'est vu refuser l'accès qu'il demandait et que le Commissaire a menacé d'avoir recours aux tribunaux pour obtenir la divulgation des renseignements en question.

Abandonnée. Le plaignant a retiré la plainte (souvent parce que le problème a été résolu avant le début de l'enquête), ou bien il n'a pas répondu aux appels ou aux lettres de suivi.

Origine des plaintes réglées par province et territoire

Terre-Neuve	3
Île-du-Prince-Édouard	35
Nouvelle-Écosse	17
Nouveau-Brunswick	165
Québec	240
Région de la Capitale nationale	
Québec	4
Région de la Capitale nationale	
Ontario	53
Ontario	200
Manitoba	21
Saskatchewan	96
Alberta	57
Colombie-Britannique	134
Territoires du Nord-Ouest	1
Yukon	0
Hors Canada	2
Total	**1028**

Dossiers

EIC peut obtenir des renseignements médicaux détaillés sur les prestataires de l'assurance-chômage

Un Ontarien s'est plaint de la quantité de renseignements médicaux que la Commission d'emploi et d'immigration du Canada a recueillis quand il a réclamé des prestations d'assurance-chômage pour raisons médicales.

Le plaignant exerçait des fonctions modifiées au moment de sa mise en disponibilité, parce qu'il avait été blessé. Il a communiqué à EIC des renseignements provenant de son médecin, qui avait précisé sa période de convalescence. Sa demande de prestations a été acceptée. Une semaine plus tard, un spécialiste a prolongé la période de convalescence du plaignant parce que sa blessure guérissait mal. Par la suite, la période de convalescence a été de nouveau prolongée. Chaque fois, le plaignant a informé EIC.

Après la deuxième prolongation, EIC a demandé au médecin de remplir un formulaire. Toutefois, les renseignements obtenus ne lui ont pas paru satisfaisants. Le médecin s'est donc vu réclamer plus de détails. Il a rempli le formulaire avec réticence, parce que ces détails étaient d'après lui protégés par le secret professionnel.

L'enquête a révélé que les deux médecins avaient fourni des renseignements contradictoires. En pareil cas, EIC a le droit d'exiger un diagnostic pour pouvoir régler la demande. Le Commissaire a conclu que les responsables d'EIC avaient agi avec prudence, conformément au règlement de l'assurance-chômage, en obtenant une corroboration des renseignements reçus. Il a considéré que la plainte n'était pas bien fondée.

Les données d'état civil sont nécessaires pour l'obtention d'un passeport

Un homme d'Ottawa s'est plaint d'avoir dû révéler son état civil actuel et passé à la personne qui s'était portée garante de sa demande de passeport. En outre, il a dit s'inquiéter de ce que les Affaires extérieures avaient recueilli trop de renseignements dans sa demande.

Les gens qui demandent un passeport doivent révéler s'ils sont mariés ou s'ils l'ont déjà été. On explique dans le formulaire que ces détails sont nécessaires pour établir l'identité, la citoyenneté ou la garde des enfants. Toutefois, l'enquête a révélé que l'information n'est indispensable que dans trois cas :

* quand le nom de famille qui figure sur le passeport a changé après le mariage de la personne (il s'agit soit du nom de famille du conjoint, soit d'une combinaison du nom de famille de la personne et de celui du conjoint);

* quand le nom des enfants est inscrit dans le passeport, (les détails fournis contribuent à la détermination de la garde légale);

* quand la personne qui demande le passeport est une femme mariée à un homme qui n'était pas sujet britannique avant le 1er janvier 1947. La femme peut avoir cessé, suite à son mariage, d'être sujette britannique et, en application des lois en vigueur à l'époque, citoyenne canadienne.

Dans tous les autres cas, les examinateurs des demandes de passeport peuvent s'abstenir de tenir compte des renseignements sur l'état civil.

Le Commissaire a reconnu que les Affaires extérieures avaient besoin de ces renseignements, mais était-il clairement indiqué sur le formulaire qu'ils n'étaient indispensables que dans les trois cas susmentionnés? Les Affaires extérieures ont consenti à expliquer la question dans un nouveau formulaire.

Le Commissaire a rejeté l'idée qu'on portait atteinte à la vie privée des gens en exigeant que les garants connaissent les détails de leur état civil. En effet, les garants ne sont pas simplement témoins de la signature des requérants; ils attestent que les renseignements fournis sont exacts, au meilleur de leur connaissance.

Le Commissaire a déclaré que, « puisqu'un passeport permet à son porteur d'entrer au Canada de plein droit, l'obligation de divulguer ces renseignements aux garants ne peut être considérée comme une exigence déraisonnable ».

Il a donc jugé la plainte non fondée.

La GRC peut communiquer des renseignements exigés par subpœna

Un avocat mêlé à une poursuite mettant en cause une compagnie d'assurance s'est plaint que la GRC avait donné à l'avocat de la compagnie une copie de la déclaration de son client à la police, sans son consentement.

La GRC a expliqué qu'elle avait parlé de cette partie du dossier avec l'avocat de la compagnie, mais qu'elle ne lui avait ni donné une copie du document, ni permis d'en consulter une. Toutefois, les renseignements en question avaient été exigés par subpœna au cours du procès au pénal d'un autre individu. La GRC a produit les renseignements exigés par ce subpoena; ils faisaient donc partie des dossiers du tribunal. Par conséquent, la GRC n'avait rien discuté qui n'ait déjà été divulgué au procès.

La plainte a été rejetée, parce que la Loi permet aux institutions gouvernementales de communiquer des renseignements personnels exigés par subpœna.

Il ne coûte rien d'invoquer la Loi sur la protection des renseignements personnels

Un homme âgé s'est plaint qu'on lui ait facturé 25 $ pour s'être prévalu de la *Loi sur la protection des renseignements personnels*. Il avait lu l'information sur la façon d'invoquer la Loi dans le *Guide des programmes et des services fédéraux pour les aîné(e)s*, une publication de Santé et Bien-être social Canada. Par la suite, il a demandé son dossier d'emploi aux Archives nationales et son dossier d'immigration à Emploi et Immigration Canada (EIC).

Les Archives nationales ont fait suivre sa demande à son ancien employeur; le plaignant a reçu les renseignements demandés peu de temps après. Toutefois, EIC lui a facturé 25 $ pour ses papiers d'immigration. Étant donné qu'il n'était pas question de frais dans le Guide, l'intéressé a écrit à Santé et Bien-être social Canada pour leur demander de le préciser à l'avenir.

Un enquêteur a constaté que le personnel d'EIC avait tout simplement mal interprété la demande. Les personnes âgées ont souvent besoin de copies certifiées de leurs documents d'entrée au pays pour étayer leurs demandes de pension. Or, EIC facture ce service. S'étant rendu compte que le plaignant ne voulait pas de copies certifiées, mais simplement consulter le dossier en vertu de la *Loi sur la protection des*

renseignements personnels, on lui a remboursé les 25 $.

La plainte était fondée.

Les évaluations de rendement doivent être conservées cinq ans

Lorsqu'un plaignant a déclaré qu'un ministère conservait trop longtemps les évaluations de rendement de ses employés, il a suscité des discussions entre Revenu Canada (Douanes et Accise), les Archives nationales, le Conseil du Trésor et le Commissaire à la protection de la vie privée.

Le plaignant a déclaré au Commissaire que Douanes et Accise conservait les évaluations de rendement plus de trois ans, malgré la période indiquée dans le *Répertoire de renseignements personnels*. La période de conservation des évaluations est fixée par les Archives nationales, de concert avec le Conseil du Trésor. Toutefois, Douanes et Accise considérait qu'il n'était pas tenu de respecter cette durée et qu'il n'y avait pas matière à plainte. Par contre, le Conseil du Trésor considérait la période comme obligatoire.

Le Commissaire a accepté d'étudier la question. Après enquête, il a été confirmé que Douanes et Accise avait bien conservé les évaluations du plaignant (comme toutes les autres) pendant plus de trois ans. Après des consultations avec Douanes et Accise, le Conseil du Trésor et les Archives nationales, l'enquêteur a constaté que le Conseil du Trésor avait porté la période de conservation à cinq ans, mais que Douanes et Accise n'avait pas été mis au courant.

Après discussion, le Ministère a conclu que l'esprit de la politique du Conseil du Trésor était clair, et il a accepté de respecter la période de cinq ans.

Les résultats des tests doivent être interprétés par des spécialistes

Une avocate qui se préparait à plaider en appel avait demandé des renseignements sur son client contenus dans deux fichiers du Service correctionnel du Canada (SCC). Elle a porté plainte quand celui-ci ne lui a pas communiqué les renseignements. L'enquête a révélé qu'une grande partie des renseignements contenus dans le fichier des dossiers médicaux des contrevenants est fournie à titre confidentiel par une province, de sorte que le SCC est tenu par la Loi de ne pas les divulguer. L'enquêteur a donc proposé à l'avocate de demander les renseignements en invoquant la loi provinciale.

Le SCC avait aussi déclaré inconsultables les données brutes des tests psychologiques conservées dans son fichier de données psychologiques, en disant que la divulgation de ces renseignements n'aurait pas bien servi les intérêts du détenu, parce que les résultats bruts auraient pu être mal interprétés par des profanes.

D'après un psychologue du SCC, le test est protégé par le droit d'auteur, et les psychologues n'ont pas le droit d'en donner de copie. En outre, si les questions, les réponses et les résultats étaient rendus publics, les tests ne seraient plus valides, particulièrement dans un milieu fermé comme un établissement pénitencier. De plus, les résultats des examens peuvent varier d'un jour à l'autre selon l'état de santé ou l'humeur des sujets. Là encore, les profanes risquent de mal interpréter les fluctuations et les résultats ponctuels.

On a conseillé à l'avocate de retenir les services d'un psychologue agréé auquel les renseignements demandés auraient pu être communiqués, en sa qualité de témoin expert.

Le Commissaire a trouvé ces arguments convaincants et il a jugé la plainte non fondée.

Les requérants n'ont pas accès aux noms des personnes consultées sur leur compte

Certains candidats à des postes de la GRC et certains anciens membres de la Gendarmerie avaient demandé des renseignements tirés de leurs dossiers de sécurité. Ils se sont plaints quand la GRC ne leur a pas communiqué les noms et les commentaires des personnes impliquées au cours des enquêtes de sécurité.

La GRC fait des enquêtes de sécurité plus poussées dans le cas des policiers que dans celui des simples fonctionnaires. En effet, les policiers ont le pouvoir d'arrêter des gens et de porter des armes à feu, de sorte que leur tempérament et leur caractère ont une importance toute particulière. Bref, la GRC a déclaré qu'elle devait protéger ses sources pour être sûre de leur franchise.

Après avoir discuté des plaintes avec l'enquêteur, la GRC a consenti à examiner les renseignements en question. Elle a conclu que les commentaires de ses sources pouvaient être divulgués, mais elle n'a pas voulu révéler leur nom ou d'autres détails grâce auxquels on aurait pu les identifier, afin de protéger l'intégrité des enquêtes.

Le Commissaire a accepté cette solution; il a jugé les plaintes bien fondées, mais résolues.

Un dossier d'hôpital datant de la Deuxième Guerre mondiale a disparu

En dépit des efforts des Archives nationales, un citoyen de la Colombie-Britannique n'a pas obtenu tous les renseignements qu'il voulait du fichier des Dossiers médicaux de la Seconde Guerre mondiale.

Le plaignant a déclaré au Commissaire que les Archives lui avaient envoyé des renseignements, mais que les documents sur son séjour dans un hôpital au cours des années 1940 manquaient. Il s'agissait notamment d'un formulaire qu'il avait été obligé de signer pour s'engager à ne pas demander de pension militaire.

À la demande d'un enquêteur, les Archives ont fait des recherches dans d'autres fichiers, mais sans succès. Elles ont trouvé les dossiers de l'hôpital (qui n'existe plus), mais pas ceux de la période du traitement du plaignant.

L'enquêteur s'est alors adressé au ministère des Anciens combattants, qui a lui aussi fait des recherches, sans réussir à trouver les dossiers manquants.

Le Commissaire a conclu que les dossiers étaient introuvables et que les Archives avaient fait de leur mieux. Il a jugé la plainte non fondée.

Non-divulgation du nom d'un informateur dans une affaire d'impôt

Une femme de Winnipeg s'était plainte à l'Institut manitobain des comptables agréés que son ancien comptable agréé avait commis une faute professionnelle. L'Institut a fait enquête et il a demandé à Revenu Canada (Impôt), au nom de la plaignante, de lui communiquer sa déclaration d'impôt sur le revenu.

Revenu Canada a refusé de divulguer certains renseignements, soit parce qu'ils concernaient une autre personne, soit parce que leur divulgation aurait nui à l'application de la *Loi de l'impôt sur le revenu*.

L'avocat intéressé a porté plainte au Commissaire.

L'enquête a révélé qu'une partie des renseignements concernait effectivement quelqu'un d'autre, de sorte que leur non-divulgation était parfaitement légitime. Le reste des renseignements portaient sur une source confidentielle. Le Commissaire a reconnu que la divulgation de ces renseignements risquait de nuire à l'application de la *Loi de l'impôt sur le revenu*. Toutefois, il a ajouté qu'on pourrait maintenir que l'intérêt public aurait été mieux servi par une divulgation des renseignements en question. Néanmoins, la *Loi sur la protection des renseignements personnels* donne au ministère en cause le droit de décider; d'après le Commissaire, Revenu Canada n'a pas abusé de ses pouvoirs en refusant de divulguer les renseignements, et il a jugé la plainte non fondée.

L'employeur comparait les registres de congés de maladie

Une femme a demandé au Commissariat si la Société canadienne des postes (son employeur et celui de son mari) pouvait se servir de son registre des présences pour enquêter sur l'absentéisme de son mari. Le dossier de la femme avait été communiqué à un superviseur dont elle ne relève pas, et le mari avait trouvé une des fiches de présence de sa femme dans son propre dossier.

L'enquête a dû déterminer s'il était admissible que la Société compare les registres des présences du couple pour vérifier les présences du mari.

La Société estimait que cette utilisation des renseignements était compatible avec la raison pour laquelle ils avaient été recueillis, puisqu'elle voulait s'assurer que les employés se servaient de leurs congés conformément à la convention collective. Selon elle, quand la direction soupçonne qu'il y a des abus, il est « naturel » qu'elle examine les registres des présences, même de deux personnes ou davantage, au besoin.

Le Commissaire a informé la Société qu'il comprenait ses raisons d'agir ainsi, mais que son geste lui semblait enfreindre la *Loi sur la protection des renseignements personnels*. Il a invité la Société à lui répondre avant de rendre sa décision finale.

La Société a répondu que la comparaison des dossiers facilite le contrôle des absences et des présences dans les cas où la direction soupçonne que les employés sont de connivence pour abuser de leurs congés. Selon elle, faute de pouvoir comparer les dossiers pour confirmer le caractère frauduleux des demandes, elle serait forcée

Plaintes par motifs et résultats

Motifs	Abandonnée	Bien fondée	Bien fondée Résolue	Rejetée	Total
Accès	16	8	69	410	503
Utilisation/Divulgation	6	8	7	29	50
Correction/annotation	0	1	6	10	17
Délais	4	317	14	79	414
Langue	0	1	0	23	24
Répertoire	0	0	0	0	0
Collecte	2	1	2	12	17
Conservation/Retrait	0	0	0	3	3
TOTAL	**28**	**336**	**98**	**566**	**1028**

d'opter pour une méthode d'enquête qui perturberait bien davantage la vie privée des employés.

Le Commissaire n'a pas été convaincu par cet argument. Il a eu du mal à accepter l'idée que des comparaisons discrétionnaires des registres des présences des conjoints, des autres membres de la famille et des partenaires de golf des employés fassent partie intégrante de la gestion des présences. Il a conclu qu'accepter le bien-fondé d'une démarche comme celle-là équivaudrait à établir des distinctions injustes contre les employés dont les parents ou les amis travaillent aussi pour la Société des postes. Il a donc recommandé à la Société de mettre fin à ces comparaisons.

La Société n'était pas d'accord, mais elle était disposée à négocier une solution. Après d'autres discussions, elle a adopté des lignes directrices pertinentes. Désormais, elle continuera d'examiner les registres des présences des employés, mais ne les comparera avec d'autres que pour produire des renseignements anonymes, au besoin, pour confirmer ou infirmer l'existence d'un absentéisme chronique déjà constaté.

Les lignes directrices imposent aussi des restrictions quant aux personnes qui peuvent consulter et comparer les registres, et à qui ils peuvent être divulgués.

Interdiction d'utiliser les dossiers d'impôt pour des motifs disciplinaires

Une vérificatrice de l'impôt congédiée pour avoir falsifié ses déclarations d'impôt sur le revenu s'est plainte au Commissaire que Revenu Canada (Impôt) avait enfreint la *Loi de l'impôt sur le revenu* et la *Loi sur la protection des renseignements personnels* en se servant de ses déclarations d'impôt pour des motifs disciplinaires.

Une semaine avant de porter plainte, la femme avait demandé à la Cour fédérale de déclarer que Revenu Canada ne pouvait pas se servir des renseignements contenus dans les déclarations d'impôt, sauf aux fins autorisées par la *Loi de l'impôt sur le revenu*. Elle avait plus particulièrement soutenu que ses déclarations d'impôt ne devaient pas être citées en preuve dans une audience sur son congédiement.

Le Commissaire a reporté sa décision jusqu'après celle de la Cour. Le juge a reconnu que, en sa qualité d'employeur, Revenu Canada n'a pas le droit de se servir des déclarations d'impôt des particuliers pour l'administration du personnel.

La *Loi sur la protection des renseignements personnels* autorise le Ministère à utiliser les renseignements personnels uniquement aux fins auxquelles ils ont été recueillis, « sous réserve d'autres lois du Parlement ». Étant donné que ce n'est pas le cas ici, et que, d'après la Cour, l'utilisation des renseignements n'était pas justifiée en vertu de la *Loi de l'impôt sur le revenu*, le Commissaire a conclu que la plainte était bien fondée.

Cela ne signifie pas que Revenu Canada ne peut pas imposer de mesures disciplinaires aux employés coupables d'évasion fiscale. Le Ministère devrait tout simplement porter plainte contre ces employés, comme il le ferait dans le cas de n'importe qui d'autre soupçonné d'évasion fiscale, puis prendre des mesures disciplinaires appropriées s'il sont jugés coupables.

On divulgue des renseignements personnels sur les opérateurs radio amateurs

Un opérateur radio amateur s'est plaint que le ministère des Communications avait divulgué des renseignements personnels sur les opérateurs radio amateurs à des associations d'opérateurs amateurs et à des éditeurs qui s'en servent pour produire des répertoires des opérateurs licenciés. Le Ministère a une base de données dans laquelle il conserve les noms et les adresses de ces opérateurs.

Le plaignant s'opposait à la divulgation de ces renseignements personnels, parce qu'il ne voulait pas devenir la cible des expéditeurs de courrier indésirable ou de voleurs en quête de matériel radio coûteux.

Saisi de la plainte, le Ministère a suspendu la communication des renseignements jusqu'à ce que le Commissaire rende sa décision. Résultat : un barrage d'appels et de lettres d'opérateurs au Ministère et au Commissariat.

L'enquête a révélé que cette divulgation est une question complexe. Les représentants du Ministère ont expliqué au Commissaire pourquoi ils la considèrent comme compatible avec les fins auxquelles les renseignements ont été recueillis.

Le Ministère est chargé de la gestion du spectre radioélectrique, une ressource publique limitée. Les personnes qui réussissent l'examen d'agrément se voient assigner un indicatif d'appel lorsqu'ils reçoivent leur licence. Comme les opérateurs sont connus publiquement, ils peuvent s'autocontrôler, étant donné que les abus et les erreurs des amateurs peuvent nuire aux autres transmissions radio. À mesure qu'on approche du point de saturation et que

les interférences électromagnétiques s'intensifient, le Ministère considère ce contrôle comme un élément important de la gestion du spectre. Il estime en outre qu'il n'est pas bon de permettre à des particuliers d'utiliser anonymement une ressource commune.

Par ailleurs, en sa qualité de membre de l'Union internationale des télécommunications, le Ministère est tenu d'offrir au public l'accès aux noms, aux adresses et aux indicatifs d'appel des opérateurs, en vertu de deux articles du règlement international, qui portent sur les enquêtes dans les cas d'interférence, la communication entre les opérateurs et leur perfectionnement personnel.

De plus, le Ministère divulgue des renseignements sur les licences pour permettre aux amateurs de communiquer entre eux, ce qui comprend la vérification des indicatifs et d'autres détails techniques. Ces mesures aident les opérateurs à s'acquitter des responsabilités qui leur incombent en vertu du Règlement général sur la radio, lequel les oblige à confirmer si un contact est un amateur licencié. Enfin, le Ministère est tenu de divulguer les noms et le statut (licencié ou pas) des amateurs utilisant des systèmes partagés (tels que des satellites), qui sont financés et maintenus par la collectivité des amateurs.

D'un autre côté, le Ministère a reconnu que les opérateurs ne tenaient pas tous à se joindre à des clubs, à se porter volontaires pour assurer des services de communication en cas d'urgence ou à figurer dans des répertoires. Néanmoins, il estime que les amateurs ne peuvent pas se soustraire à leur responsabilité de rendre publique leur utilisation du spectre.

Le Commissaire a accepté les arguments bien étoffés que le Ministère lui a présenté pour justifier la divulgation des renseignements, en soulignant que les opérateurs peuvent demander aux éditeurs de répertoire du secteur privé de ne pas publier les renseignements qui les concernent. Il a jugé la plainte non fondée.

Le secret professionnel d'un avocat va loin!

Une femme mêlée à une poursuite pour congédiement injuste intentée contre Transports Canada avait demandé les renseignements qui la concernaient dans les 20 fichiers ordinaires des employés du Ministère. Elle a porté plainte au Commissaire, en disant que la réponse avait tardé à venir et qu'il manquait des renseignements.

L'enquête a révélé que 14 des fichiers ne contenaient pas de renseignements sur l'intéressée. Il était aussi évident que Transports Canada n'avait pas communiqué certains renseignements qui figuraient dans le dossier de grief de la plaignante, soit parce qu'ils concernaient quelqu'un d'autre, soit parce que le Ministère considérait qu'ils étaient protégés par le secret professionnel d'un avocat.

L'enquêteur a découvert que Transports Canada avait refusé de communiquer sa demande d'opinion juridique, l'opinion juridique elle-même et toute la documentation pertinente. Le Ministère avait conservé cette documentation, qui fait normalement partie du dossier de grief, pour obtenir une opinion juridique. Selon lui, une fois que ces renseignements ont été joints à une demande de conseils juridiques, ils sont protégés par le secret professionnel d'un avocat.

Pourtant, la jurisprudence est claire : le secret professionnel d'un avocat s'applique aux communications entre les parties et aux documents créés ou obtenus expressément dans le contexte d'un litige. Les documents qu'un client confie à un conseiller juridique ne sont pas tous protégés par le secret professionnel. Par exemple, les faits obtenus d'autres sources, sans l'être pour l'avocat ou par celui-ci, ne sont pas protégés.

Le Commissaire a informé Transports Canada qu'il considérait que c'était donner à la notion de secret professionnel une extension inacceptable. Il a recommandé que les documents contenus dans le dossier de grief soient divulgués, ce qui a amené le Ministère à divulguer une partie des renseignements. Le Commissaire a alors proposé à la plaignante de porter elle-même sa cause à la Cour fédérale. Elle a accepté, et le Commissaire en a informé Transports Canada, qui avait entre-temps reçu un avis du ministère de la Justice, et qui a décidé de divulguer les renseignements demandés. Le Commissaire a jugé la plainte bien fondée.

Demandes de renseignements

Le nombre de demandes a presque doublé cette année; le Commissariat en a reçu 2041, comparativement à 1248 l'an dernier. Une agente à temps plein reçoit la majorité des appels et son système efficace d'inscription des demandes fait paraître l'augmentation plus importante qu'elle ne l'est en réalité. Auparavant, on ne comptait tout simplement pas certaines demandes; le personnel y répondait sans prendre le temps de les consigner.

Les questions sont très variées. Elles peuvent être aussi simples que de vouloir savoir à quel ministère ou organisme s'adresser pour avoir accès à des renseignements personnels (environ 8 p. 100 des demandes).

D'autres demandes peuvent prendre un temps fou, mais se révéler très enrichissantes, comme l'appel d'un député sur un questionnaire détaillé que les auxiliaires temporaires de la Société des postes ont dû remplir avant d'être embauchés pour livrer du courrier publicitaire. Après discussion avec le Commissariat, la Société a cessé d'utiliser ce questionnaire. Les demandes de renseignements sur l'utilisation et l'interprétation de la *Loi sur la protection des renseignements personnels* représentent 46 p. 100 du total.

Les questions et les plaintes sur l'utilisation du NAS (numéro d'assurance sociale) se sont multipliées cette année, jusqu'à concurrence de 21 p. 100 du total des demandes de renseignements. Cette augmentation est largement imputable à une modification de la *Loi de l'impôt sur le revenu* qui oblige les particuliers à donner leur NAS à leurs institutions financières. Certains des gens qui ont communiqué avec le Commissariat se sont indignés de la contradiction qu'ils trouvaient entre la nouvelle politique gouvernementale de restriction de l'utilisation du NAS et cette obligation de le donner aux banques, compagnies de fiducie, coopératives de crédit, caisses populaires et maisons de courtage. Les agents du Commissaire ont dû leur préciser qu'ils étaient aussi tenus de le donner aux agents d'immeubles qui mettent des chèques de dépôt en banque et aux agents d'assurance.

D'autres personnes étaient mécontentes de ce qu'elles considéraient comme le « secret » qui avait entouré l'introduction de cette nouvelle obligation. En fait, comme nous l'avons précisé, les modifications à la *Loi de l'impôt sur le revenu* ont été adoptées conformément à la procédure parlementaire normale. Les députés n'ont pas soulevé de questions sur cette nouvelle obligation de produire le NAS, et la presse n'en n'a pas fait état. La plupart des gens qui ont communiqué avec le Commissariat à ce sujet ont été mis au courant de cette nouvelle obligation et de l'amende qu'ils devraient payer à défaut de donner leur NAS quand ils ont acheté leur nouvelle émission d'obligations d'épargne du Canada ou qu'ils sont allés à la banque... et ils n'ont pas été très contents.

Environ 10 p. 100 des gens qui demandaient des renseignements déplorent que certaines institutions fédérales ne soient pas assujetties à la *Loi sur la protection des renseignements personnels*. (Il s'agit souvent de sociétés d'État, comme Air Canada et le Canadien National.) Un certain nombre de sociétés d'État devraient être assujetties à la Loi en 1989.

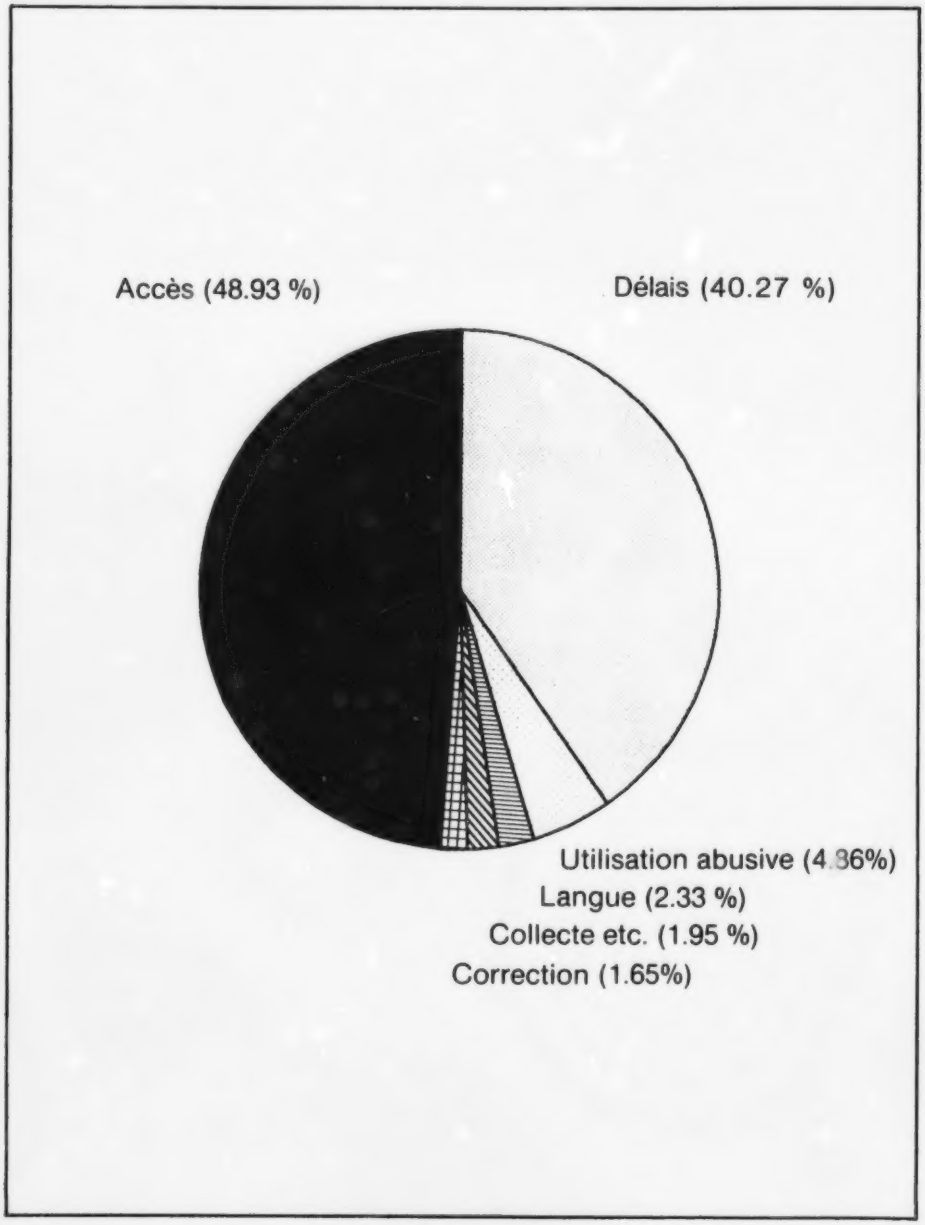
Plaintes réglées par institution, motifs et résultats

Ministère	Nombre	Bien-fondée	Bien-fondée - Résolue	Non-fondée	Abandonnée
Affaires des anciens combattants Canada	3	0	0	3	0
Affaires extérieures Canada	14	3	1	10	0
Affaires indiennes et du Nord Canada	1	0	1	0	0
Agriculture Canada	5	0	2	3	0
Archives nationales du Canada	15	1	0	14	0
Bureau de l'enquêteur correctionnel	1	0	1	0	0
Bureau de l'Inspecteur général du service canadien du renseignement de sécurité	4	0	0	4	0
Bureau du Conseil privé	6	0	1	5	0
Bureau du Directeur général des élections	1	0	0	1	0
Comité de surveillance des activités de renseignement de sécurité	4	0	0	4	0
Commissariat aux langues officielles	3	0	0	3	0
Commission canadienne des droits de la personne	11	0	2	9	0
Commission de la Fonction publique	8	0	4	3	1
Commission nationale des libérations conditionnelles	30	3	11	15	1
Communications, Ministère des	2	1	1	0	0
Conseil canadien des relations de travail	1	0	0	1	0

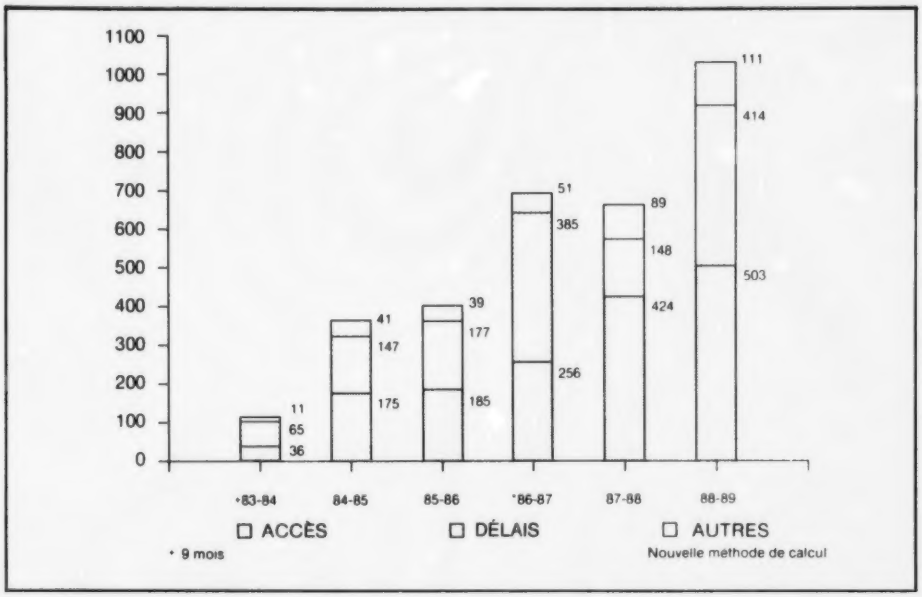
Plaintes réglées par institution, motifs et résultats (suite)

Ministère	Nombre	Bien-fondée	Bien-fondée - Résolue	Non-fondée	Abandonnée
Consommation et Corporations Canada	1	0	0	1	0
Défense nationale	85	32	4	46	3
Emploi et Immigration Canada	68	24	13	28	3
Energie, Mines et Ressources Canada	2	1	1	0	0
Environnement Canada	3	0	0	0	3
Gendarmerie royale du Canada	109	13	6	86	4
Justice Canada, Ministère de la	5	0	0	5	0
Revenu Canada - Douanes et Accise	15	5	1	9	0
Revenu Canada - Impôt	37	11	0	21	5
Santé et Bien-être social Canada	18	3	5	8	2
Service canadien du renseignement de sécurité	49	3	6	40	0
Service correctionnel Canada	404	203	29	168	4
Société canadienne d'hypothèque et de logement	1	0	1	0	0
Société canadienne des ports	4	0	4	0	0
Société canadienne des postes	12	2	2	7	1
Solliciteur général Canada	22	0	0	22	0
Transports Canada	77	31	2	43	1
Travail Canada	5	0	0	5	0
Travaux publics Canada	2	0	0	2	0
TOTAL	**1028**	**336**	**98**	**566**	**28**

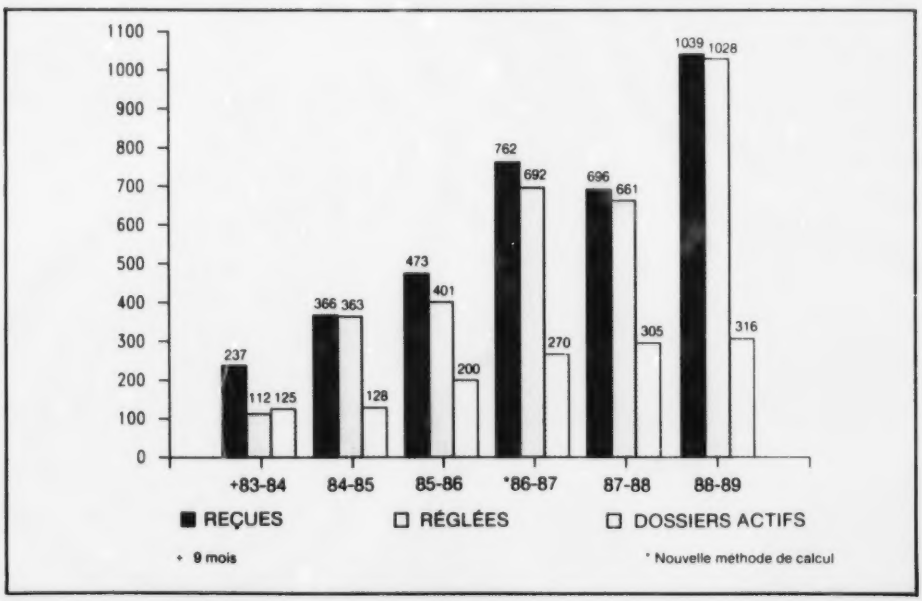
Plaintes réglées par motifs 1988-1989



Plaintes régleés et motifs 1983-1989



Nombre de dossiers 1983-1989



Enfin, 15 p. 100 des demandes portent sur des questions de protection de la vie privée dans le secteur provincial ou privé, qui ne sont pas du ressort du Commissariat. Par exemple, une Ontarienne a téléphoné au Commissariat pour savoir si la *Loi sur la protection des renseignements personnels* pouvait empêcher les autorités municipales de vendre leur liste d'électeurs à des entreprises ou à des particuliers. Le Commissariat n'a pas pu faire enquête, étant donné que les municipalités ne relèvent pas de la Loi. Elles ne seront d'ailleurs pas assujetties à la législation provinciale avant 1991. (Il est interdit de vendre les listes électorales fédérales.)

Direction générale de l'observation

Institutions ayant fait l'objet d'une vérification

Le Commissariat a choisi les organismes devant faire l'objet d'une vérification en fonction des risques globaux que ceux-ci présentaient, mesurés aussi objectivement que possible.

Les vérifications ont porté sur la Société canadienne des postes, le Secrétariat du Solliciteur général et Emploi et Immigration Canada, ainsi que sur des institutions de taille plus réduite, à savoir le ministère des Finances, la Commission d'appel des pensions et le Conseil des sciences du Canada.

Le Commissariat termine actuellement des vérifications dans les organismes suivants : La Commission de réforme du droit, Le Centre de recherches pour le développement international, la Commission d'examen des exportations de biens culturels, la Société pour l'expansion des exportations et la Société canadienne des brevets et d'exploitation Ltée.

Méthode de vérification

Les vérifications sont confiées à des équipes de deux à quatre enquêteurs qui visitent un certain nombre de services de l'administration centrale et plusieurs bureaux régionaux des ministères et organismes visés. Ils examinent un échantillon de dossiers prélevés au hasard dans certains fichiers et interrogent les cadres et les employés qui utilisent et gèrent ces dossiers.

La vérification porte sur les aspects suivants :

* la collecte, l'usage, la divulgation, la conservation, le retrait et la sécurité des renseignements personnels;
* la qualité des lignes directrices internes et l'observation par le ministère ou l'organisme intéressé de la politique et des directives sur les renseignements personnels établies par l'organisme central;
* l'exactitude et le caractère exhaustif du contenu du Répertoire de renseignements personnels du ministère ou de l'organisme;
* la connaissance qu'a le personnel de la *Loi sur la protection des renseignements personnels* et de ses implications pour le traitement de ces renseignements;
* l'accès des particuliers aux renseignements personnels les concernant;
* la délégation des pouvoirs par le responsable du ministère ou de l'organisme.

Une fois la vérification terminée, les enquêteurs parlent avec les cadres de leurs constatations, en insistant sur les lacunes relevées. Le ministère (ou l'organisme) reçoit d'abord un projet de rapport, puis un rapport final. Conformément à la pratique courante de vérification, les rapports ne portent que sur les points à corriger.

Vérification du travail des vérificateurs

Bien entendu, six vérificateurs ne sauraient en si peu de temps enquêter sur tous les organismes gouvernementaux assujettis à la *Loi sur la protection des renseignements personnels*. Par conséquent, le Commissaire a toujours pressé les vérificateurs internes des ministères et organismes de veiller à la protection de la vie privée. L'année écoulée a révélé des efforts encourageants en ce sens.

Emploi et Immigration Canada a bien répondu à l'appel. Après avoir consulté le Commissariat, le Bureau de la vérification interne de la Commission a entrepris un examen de la façon dont EIC traite les renseignements personnels. Le Commissariat a par la suite étudié les documents de travail des vérificateurs internes pour déterminer le niveau de confiance qu'ils pouvaient attribuer à la vérification. L'examen a révélé un travail de qualité tout à fait professionnelle, que le Commissaire peut accepter avec une confiance égale à celle qu'il accorderait à un rapport de ses propres vérificateurs. (Les constatations sont résumées plus loin.)

Constatations

Certaines constatations valent pour tous les ministères et organismes visés. Par exemple, rares sont les employés d'autres services que ceux de l'accès à l'information et de la protection de la vie privée qui connaissent leurs droits en vertu de la *Loi sur la protection* des renseignements personnels, ou qui comprennent leurs responsabilités pour la collecte, la conservation, l'usage, la divulgation et le retrait des renseignements personnels.

En outre, ces renseignements sont généralement mal protégés. Les employés des services opérationnels (et même certains de ceux des services de sécurité) ne comprennent pas encore parfaitement la nouvelle politique gouvernementale sur la sécurité, et plus particulièrement ses dispositions portant sur la protection des renseignements personnels. Néanmoins, les vérificateurs n'ont trouvé aucun indice permettant de croire que la confidentialité de ces renseignements ait été menacée.

Cette année encore, les vérificateurs ont constaté que certains dossiers contenant des renseignements personnels n'ont pas été identifiés et décrits correctement dans le *Répertoire de renseignements personnels*. De même, certains usages des renseignements personnels que l'institution considérait comme « compatibles » avec les fins auxquelles ils avaient été recueillis ne figuraient pas dans les descriptions du Répertoire.

Les vérifications ont fait ressortir la nécessité d'une politique applicable à l'ensemble de l'administration fédérale et précisant qui devrait être autorisé à consulter les dossiers de renseignements personnels. Cette politique devrait tenir compte des subtilités de la *Loi sur la protection des renseignements personnels* et limiter la quantité de renseignements de ce genre dont les cadres ont besoin pour s'acquitter des exigences légitimes de leurs postes. La présentation actuelle de la plupart des dossiers du personnel fait qu'il est impossible de cloisonner les renseignements en fonction du principe du besoin de savoir.

Sécurité et protection de la vie privée : un mariage difficile

La plupart des employés traitent la sécurité en matière d'information comme le fief des agents de sécurité ou des spécialistes de l'information de gestion. Or, la formation que ces gens ont reçue les pousse à définir la sécurité dans le contexte de « l'intérêt national » et non de la vie privée des particuliers. Souvent, ils ne savent pas comment réagir à la cote « protégé », qu'on applique désormais à tous les renseignements personnels qui ne sont pas d'intérêt national.

Le Conseil du Trésor, le Centre de sécurité des télécommunications, la GRC et le Commissariat ont fait de grands efforts pour sensibiliser les employés à la protection des renseignements personnels, rarement considérés jusqu'à présent comme étant vulnérables, du point de vue de la sécurité.

Grâce à des échanges réguliers, les quatre organismes ont défini des niveaux de protection correspondant au caractère délicat des renseignements personnels. Ces niveaux seront inclus dans la nouvelle politique du gouvernement sur la sécurité. La publication et l'application de ce nouveau document de principe devraient aider les ministères et organismes à appliquer des normes de sécurité pour tous les renseignements désignés.

Enquêtes sur des incidents

Le Commissariat a enquêté cette année sur la perte d'un document et joué les observateurs dans l'enquête qu'un ministère a menée sur des dossiers perdus. L'enquête a porté sur la perte de microfiches d'impôt au bureau de district de Revenu Canada (Impôt) à Calgary. En octobre 1988, Revenu Canada a informé le Commissaire qu'il avait perdu 38 feuilles d'un jeu de microfiches. Ces feuilles contenaient des renseignements permettant d'identifier des employeurs (grâce à un code numérique) et leurs employés (noms de famille, initiales, numéros d'assurance sociale, revenus, pensions, contributions à l'assurance chômage et autres retenues à la source). Chaque feuille pouvait contenir des données sur plus de 8 000 personnes.

L'enquête a commencé à l'administration centrale du Ministère, à Ottawa. Les enquêteurs ont retracé la procédure de production et d'envoi des jeux de microfiches, ce qui les a convaincus que le jeu était arrivé intact à destination.

Ensuite, les enquêteurs ont suivi la piste des fiches jusqu'au bureau de district de Calgary. Une fois que le jeu a été ouvert et que les fiches ont été comptées, elles ont été mises dans un boîtier auquel environ 150 employés avaient accès pendant la journée. La nuit, les fiches étaient gardées sous clé dans une armoire, mais les clés étaient dans un tiroir de bureau non verrouillé. Le matin, le premier employé qui avait besoin des fiches pouvait déverrouiller l'armoire et mettre les fiches dans le boîtier. On n'a jamais pu savoir qui avait sorti le jeu de l'armoire le jour où la perte a été constatée. Les 38 fiches n'ont jamais été retrouvées.

Les enquêteurs se sont rendu compte que les employés pouvaient sortir des fiches du jeu et les emporter dans d'autres locaux de l'étage sans signer de registre. Seuls les employés ne travaillant pas dans le service en question étaient tenus de signer un registre pour en sortir des fiches.

Tout compte fait, les enquêteurs ont jugé que les mesures de sécurité de Revenu Canada étaient suffisantes pour la production et la distribution des microfiches et que les employés étaient très sensibilisés aux questions de sécurité. Toutefois, une fois rendus dans un bureau « sûr », ils semblaient négliger la nécessité de protéger les renseignements personnels; le fait que la clé de l'armoire était dans un tiroir non verrouillé le montre bien. En outre, les employés ignoraient à peu près tout de la *Loi sur la protection des renseignements personnels* et des obligations qu'elle impose au personnel utilisant des renseignements de ce genre.

À la suite de l'incident, le Bureau du Calgary a adopté de nouvelles procédures plus strictes. Les jeux de fiches et les lecteurs sont désormais conservés et utilisés dans une pièce sûre qui n'est jamais déverrouillée sans qu'il y ait quelqu'un à l'intérieur. Les employés doivent inscrire dans un registre les fiches qu'ils veulent utiliser; on les sort du jeu de fiches, puis on remet le jeu dans l'armoire verrouillable. En outre, on utilise des mesures de contrôle radicales pour la destruction des vieilles fiches.

Ces nouvelles mesures rendent inutiles les recommandations que le Commissariat aurait pu faire à Revenu Canada pour l'amener à resserrer la sécurité dans ses services de Calgary. Toutefois, le Commissaire a recommandé au Ministère d'ordonner à ses autres bureaux de modifier leurs méthodes d'entreposage et de traitement des microfiches de façon à respecter la *Loi sur la protection des renseignements personnels* et la nouvelle politique du gouvernement sur la sécurité. En outre, il a répété plusieurs des recommandations qu'il avait faites après le vol de microfiches qui avait eu lieu au bureau de Toronto du Ministère (Rapport annuel 1986–1987) :

* les employés devraient être sensibilisés à leur obligation de protéger les renseignements personnels en vertu de la *Loi sur la protection des renseignements personnels;*

* les microfiches devraient être protégées plus étroitement encore que les dossiers sur support papier et

* le personnel ne devrait avoir accès aux microfiches que s'il en a vraiment besoin.

Le second incident est le suivant : le Service correctionnel du Canada a perdu plus de 30 caisses de vieux dossiers de détenus pendant leur transport jusqu'au Centre des dossiers des Archives nationales, en Colombie-Britannique.

L'entreprise de camionnage responsable a cherché les caisses pendant près de deux semaines avant de les retrouver dans son entrepôt. Les caisses ne semblaient pas avoir été ouvertes, mais l'incident aurait pu être évité si l'on avait pris des mesures de sécurité normales.

Les vérifications

Deux des vérifications réalisées cette année ont révélé une anomalie qui pourrait causer des problèmes, et qui a entraîné des discussions entre le Commissariat et les organismes en cause, la Société canadienne des postes et la Société pour l'expansion des exportations, deux sociétés d'État qui sont assujetties à la *Loi sur la protection des renseignements personnels* et qui, en théorie, ne sont pas liées par la politique du gouvernement du Canada sur la sécurité. L'une et l'autre ont choisi de respecter les dispositions de la politique en matière d'intérêt national, mais elle se sont opposées à ce que le Commissariat s'en serve comme normes d'évaluation de leurs mesures de sécurité matérielle.

Le Commissaire ne croit pas que les sociétés d'État devraient nécessairement être liées par la politique du gouvernement, mais il estime que les normes gouvernementales sont un critère raisonnable d'évaluation de leurs mesures de sécurité.

Société canadienne des postes

Les vérificateurs ont visité l'administration centrale de la Société, à Ottawa, ainsi que les bureaux divisionnaires centraux d'Edmonton, de London et de Québec.

Constatations

Connaissance de la Loi sur la protection des renseignements personnels : Comme c'est le cas dans la plupart des organismes gouvernementaux qui ont fait l'objet d'une vérification, le personnel ne comprenait pas ses droits ou ceux d'autrui — pas plus que ses responsabilités — en fonction de la *Loi sur la protection des renseignements personnels*. La Société publie régulièrement des rappels dans ses bulletins internes, mais la plupart des employés ne s'en souvenaient pas. Autrement dit, la diffusion de ces messages est insuffisante, ou leur effet est médiocre.

La Société compte mettre sur pied un programme de communication à l'appui de sa politique générale sur la protection des renseignements personnels.

Contenu du Répertoire de renseignements personnels :

1. La description de deux fichiers sur les droits de la personne (SPC/P-PU-096 et P-PE-809) ne faisaient pas état des cas de harcèlement personnel contenus dans les dossiers. La description du fichier a été modifiée en conséquence.

2. Les cartes de changement d'adresse sont désormais décrites comme une « catégorie » de renseignements personnels. Toutefois, la *Loi sur la protection des renseignements personnels* dispose que les renseignements personnels utilisés à des fins administratives doivent être inclus dans un « fichier ». Étant donné que les cartes sont utilisées pour réadresser le courrier des clients (à des fins administratives), la Société des postes créera un nouveau fichier qui contiendra les avis

de changement d'adresse. Un autre fichier a été constitué pour répondre aux autres ministères cherchant à localiser les particuliers qui sont débiteurs de l'État.

Protection des renseignements personnels : Les employés des bureaux divisionnaires centraux qui veulent consulter leur dossier personnel doivent le demander par l'intermédiaire de leur superviseur, puis consulter le dossier en sa présence. Les superviseurs ont donc accès à tous les renseignements personnels figurant aux dossiers des employés, y compris des détails tels que leurs antécédents médicaux, leurs dons à des œuvres de charité et leur état civil. Il n'est pas nécessaire d'avoir accès à des renseignements de ce genre pour superviser. La Société des postes réétudiera ses procédures d'accès aux renseignements personnels et les corrigera.

Certains dossiers personnels de l'administration centrale contenaient des renseignements limités sur d'autres employés, habituellement dans des listes où figuraient des noms et des numéros d'assurance sociale. Les renseignements portant sur des tiers seront éliminés à mesure qu'on sortira les dossiers pour s'en servir.

À Edmonton, les vérificateurs ont trouvé des renseignements personnels sur du papier de rebut dont on se débarrassait en l'envoyant à une entreprise privée qui le gardait à l'extérieur, sans protection. La Société des postes demandera aux Archives nationales de lui donner des moyens de se défaire en toute sécurité des déchets à caractère délicat, dans toute la mesure du possible. Dans les autres régions, elle assurera elle-même le retrait de ses documents.

Les enquêteurs ont aussi constaté des difficultés liées à l'élimination d'autres déchets et à la protection des armoires ou des pièces contenant des dossiers personnels. La Société des postes est déterminée à corriger ces lacunes lorsqu'elle mettra en œuvre ses nouvelles politiques sur la protection des renseignements personnels et sur la sécurité.

À Ottawa et à Edmonton, le fichier de réclamations pour la gestion des risques est partagé avec des ajusteurs d'assurances du secteur privé. Toutefois, aucune entente officielle n'a été conclue avec la compagnie d'assurance pour protéger ces renseignements conformément à la *Loi sur la protection des renseignements personnels*. La Société des postes obtiendra des ajusteurs d'assurances l'engagement de respecter l'esprit et la lettre de la Loi. Elle devra aussi décider s'il serait préférable qu'elle ajoute des dispositions sur la protection des renseignements personnels et sur la sécurité à ses contrats avec tous les agents qui recueillent ou qui reçoivent des renseignements personnels en son nom.

Usage indu des renseignements personnels : Les enquêteurs ont trouvé un manuel de formation sur les droits de la personne qui contenait des dossiers de griefs, des plaintes et des rapports d'enquêtes réels. Ces documents ont été modifiés de façon à préserver l'anonymat des intéressés.

Divulgation indue : La Société des postes a partagé sa liste de distribution de philatélistes avec la Monnaie Royale canadienne et avec d'autres expéditeurs ayant une bonne réputation. La Société était d'avis qu'il s'agissait là d'un « usage compatible » des renseignements en question. Le Commissaire n'a pour sa part pas établi de rapport logique entre le fait d'être philatéliste et celui de collectionner des pièces de monnaie ou d'autres articles. Le partage de la liste avait déjà cessé. (Il s'agit d'un cas isolé.)

Conservation et retrait : les enquêteurs ont fait plusieurs recommandations sur l'entreposage ou le retrait de dossiers personnels qui avaient été conservés trop longtemps ou trop peu de temps. (En vertu de la Loi, ils doivent être conservés au moins deux ans.) La Société des postes prendra des mesures en réponse à chacune des recommandations.

Enfin, les enquêteurs ont trouvé des empreintes digitales dans des dossiers personnels de chacune des divisions qu'ils ont visitées. Il semble que la Société prenait les empreintes digitales de tous ses employés. Le Commissaire s'est dit d'avis que les empreintes dont elle n'a plus besoin devraient être rendues aux intéressées. Celles dont la Société a encore besoin devraient être conservées dans des dossiers d'autorisations sécuritaires et de vérification de la fiabilité.

Commission d'appel des pensions

La Commission d'appel des pensions entend des appels interjetés des décisions du Régime de pensions du Canada et du Régime des rentes du Québec. Tous les dossiers sont conservés à Ottawa et tous les renseignements personnels sont sur support papier. Il n'y a pas de fichier informatique.

Constatations

Connaissance de la Loi sur la protection des renseignements personnels : Le personnel ignore à peu près tout de la Loi. La direction lui donnera la formation nécessaire.

Contenu du Répertoire de renseignements personnels : D'après le Répertoire, la *Loi sur la protection des renseignements personnels* ne s'applique pas aux documents que la Commission détient au sujets d'appels portant sur le Régime des rentes du Québec. C'est faux : tous les renseignements personnels que la Commission détient sont assujettis à la *Loi sur la protection des renseignements personnels*. La Commission modifiera le texte en conséquence.

Les enquêteurs ont constaté que le fichier des Dossiers individuels sur le personnel (CAP/P-PE-801) relève de Santé et Bien-être social Canada plutôt que de la Commission. La description du fichier sera transférée sous Santé et Bien-être social Canada; on ajoutera à la rubrique de la Commission une déclaration renvoyant les employés au Ministère. La Commission compte aussi créer un fichier intitulé « Personnel » dans lequel elle conservera les renseignements généraux sur le personnel.

Protection des renseignements personnels : Pendant la vérification, les enquêteurs ont trouvé des clés dans les serrures de classeurs contenant des dossiers complets. Ces classeurs sont dans le bureau central, et les préposés au nettoyage y ont accès pendant la soirée. La Commission veillera à ce que le personnel ne laisse plus traîner les clés. Les enquêteurs ont aussi recommandé de nouvelles procédures de destruction des déchets posant des problèmes de sécurité.

Conservation et retrait : Il n'y a pas de période de conservation avant destruction prévue pour les dossiers d'appel, dont certains datent de 1967. La Commission demandera aux Archives nationales de lui recommander une période de conservation appropriée.

Collecte de renseignements personnels : Les enquêteurs ont constaté que la Commission reçoit toutes les décisions du Comité de révision du Régime de pensions du Canada, avec les pièces, qu'un appel ait été interjeté ou pas. S'il n'y a pas d'appel, la Commission renvoie les pièces, mais conserve la décision. Le Commissaire s'est dit d'avis que cela constitue une collecte de renseignements débordant le mandat de la Commission. Celle-ci modifiera sa procédure d'examen des dossiers du Comité de révision.

Conseil des sciences du Canada

Le Conseil des sciences du Canada évalue les ressources, le potentiel et les besoins scientifiques et technologiques du Canada; il a pour mission de sensibiliser le public aux sciences et à la technologie.

Tous les dossiers du Conseil sont dans ses bureaux d'Ottawa. Les renseignements personnels ne sont pas conservés dans des fichiers informatiques ou sur microfiches.

Constatations

Connaissance de la Loi sur la protection des renseignements personnels : Le personnel du Conseil a une connaissance générale des principes de la protection de la vie privée, ce qui est rare pour une institution gouvernementale. (Le Conseil a fait des recherches sur des questions liées à la protection de la vie privée.)

Protection des renseignements personnels : Les enquêteurs ont constaté que certains employés qui utilisaient des renseignements personnels n'avaient pas fait l'objet de l'enquête de fiabilité requise par la politique du gouvernement sur la sécurité. Le Conseil a commencé à faire enquête sur tous les employés utilisant des renseignements protégés.

Les préposés au nettoyage peuvent circuler sans surveillance dans le bureau du personnel après les heures de travail. Personne ne vérifie si la porte du bureau est verrouillée après leur départ. Le Conseil précisera aux commissionnaires comment faire les vérifications qui s'imposent.

Contenu du Répertoire de renseignements personnels : Deux groupes de dossiers contenant des renseignements personnels sur des employés contractuels et sur les membres du Conseil ne sont pas décrits dans le Répertoire. Le Conseil les décrira dans la prochaine édition.

Ministère des Finances

Le Ministère est responsable de la mise en œuvre de politiques et de programmes financiers et économiques. Ses 800 employés sont tous dans ses bureaux d'Ottawa.

Constatations

Connaissance de la Loi sur la protection des renseignements personnels : Aux Finances comme ailleurs, les employés interrogés ignoraient à peu près tout de la Loi, même si le Ministère s'est donné des procédures à cet égard dès 1983 et qu'il les a complétées depuis par des séances d'information régulière. Les responsables préparent de nouvelles procédures et des lignes directrices qui seront distribuées à la Direction de l'administration et au cabinet de chaque sous-ministre adjoint.

Protection des renseignements personnels : Les vérificateurs ont constaté que les superviseurs et les employés chargés de la formation en langues officielles pouvaient consulter les dossiers du personnel sans aucune restriction, même si ni les uns ni les autres n'avaient vraiment besoin de connaître leur contenu. En outre, certains dossiers contenaient des renseignements sur d'autres employés. Dans l'un deux, on a même trouvé une évaluation dérogatoire d'un autre employé.

Le Ministère cherche des moyens de cloisonner ces dossiers pour en retirer les renseignements à caractère délicat sans entraver les superviseurs et les employés des services linguistiques dans l'exercice de leurs fonctions.

Par ailleurs, les vérificateurs ont trouvé des clés de classeurs dans des tiroirs de bureau non verrouillés et des renseignements personnels sur du papier de rebut dans des poubelles et des contenants de papier recyclable.

Les employés responsables conserveront désormais les clés sur eux et les documents contenant des renseignements personnels devront être jetés dans des sacs de déchets à brûler.

Le Ministère a accepté la proposition des enquêteurs de verrouiller les classeurs et les pièces contenant des dossiers de demandes en vertu de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels* quand les employés s'absenteront ou qu'ils quitteront le travail.

Contenu du Répertoire de renseignements personnels : Le Ministère conserve des dossiers sur les résultats des vérifications de la fiabilité de ses employés, mais il n'en fait pas état dans le *Répertoire*. Par conséquent, les employés ne peuvent demander qu'on leur donne accès à ces renseignements, étant donné qu'ils n'en connaissent pas toujours l'existence.

Le Conseil du Trésor a modifié la description de ce fichier (l'un des fichiers ordinaires que conservent tous les ministères). Les Finances adopteront la description du Conseil du Trésor.

Secrétariat du Solliciteur général

Le Secrétariat est un service du Solliciteur général qui est responsable de la Gendarmerie royale du Canada, du Service canadien du renseignement de sécurité, du Service correctionnel du Canada et de la Commission nationale des libérations conditionnelles. Les vérificateurs ont visité l'administration centrale du Secrétariat, à Ottawa.

Constatations

Protection des renseignements personnels : Les vérificateurs ont constaté beaucoup de lacunes du genre de celles qui ont été relevées dans les autres ministères et organismes : les superviseurs ont accès à des dossiers personnels détaillés; il y a des listes d'employés, certaines avec le numéro d'assurance sociale des intéressés, dans les dossiers personnels d'autres employés; les dossiers sont conservés dans des classeurs verrouillés, mais les clés sont laissées dans des tiroirs de bureau ouverts; des documents contenant des renseignements personnels sont jetés à la poubelle et des classeurs ne sont pas verrouillés quand les responsables sont absents. En outre, les couvertures des dossiers conservés dans le fichier des dossiers personnels des employés ne portent pas de mention de sécurité ou de désignation «Protégé ».

Le Secrétariat a consenti à étudier la question de la limitation de l'accès aux dossiers personnels. Il rappellera aussi à ses employés leurs responsabilités en matière de sécurité. Enfin, il utilise désormais des chemises « Protégé » pour les nouveaux dossiers personnels (ou pour les anciens, sur demande), même s'il estime qu'il ne serait pas faisable d'utiliser ce genre de chemise pour tous les dossiers existants.

Les dossiers personnels contenant des renseignements personnels de nature délicate devraient être convenablement identifiés, parce que la vérification a révélé que certains renseignements avaient été divulgués à l'extérieur de l'organisation qui les avait produits ou recueillis.

Enfin, bien que le Secrétariat ait une procédure de sécurité satisfaisante, les enquêteurs ont constaté que certains employés quittaient leur bureau sans le verrouiller.

Divulgation indue : Un manuel des ressources humaines contient des exemples qui sont des copies de documents réels (formules remplies et notes de service). Des personnes sont nommées dans ces documents. La direction a accepté d'éliminer les détails pertinents.

Conservation et retrait : Les dossiers personnels des employés et les dossiers personnels et administratifs de la GRC sont conservés au-delà de la période approuvée. Le fichier des Dossiers sur la sécurité nationale (P-PU-026) ne fait l'objet d'aucune norme de destruction. Le Secrétariat a consenti à passer les dossiers personnels en revue chaque année, et il a consulté les Archives nationales et le Service canadien du renseignement de sécurité au sujet du retrait des autres dossiers.

Contenu du Répertoire de renseignements personnels : Les dossiers des vérifications de fiabilité des employés sont conservés dans le fichier des Autorisations sécuritaires (P-SE-909) du Secrétariat, sans être décrits dans le *Répertoire*. Plusieurs fichiers ont un numéro d'approbation des Archives nationales, mais sans que la période de

conservation des renseignements ne soit précisée. À l'avenir, les vérifications de fiabilité seront conservées dans le nouveau fichier ordinaire établi par le Conseil du Trésor. Ce fichier sera décrit dans la prochaine édition du *Répertoire*, et les normes de destruction des autres fichiers le seront aussi.

Une vieille histoire : En 1986, le Solliciteur général adjoint a accepté d'éliminer les renseignements personnels contenus dans les dossiers de l'un des fichiers du Secrétariat, celui de la Protection de la vie privée (P-PU-035). Ce fichier devait par la suite être retiré du *Répertoire*. La vérification a révélé que le fichier est toujours inscrit au *Répertoire* et que 200 seulement des 600 dossiers qu'il contient ont été épurés. Le Secrétariat a promis au Commissaire que le nécessaire sera fait d'ici septembre 1989.

Emploi et Immigration Canada (EIC)

La vérification interne

La vérification a comporté deux volets : le premier, qui a été réalisé par le Bureau de la vérification interne d'EIC, a été axé sur la protection des renseignements personnels concernant les clients d'EIC. Le Commissariat a évalué le travail des vérificateurs internes. Au cours des deux prochaines années, le Bureau de la vérification interne d'EIC examinera les fichiers de renseignements personnels et les renseignements contenus dans les fichiers informatiques.

Le second volet, réalisé par le Commissariat, a porté sur les dossiers du Programme d'aide aux employés (PAE) d'EIC.

Le groupe de vérification interne s'était donné des objectifs plus vastes que ceux des vérificateurs du Commissariat, étant donné qu'EIC voulait évaluer l'efficacité de son administration et de ses structures internes d'application de la *Loi sur la protection des renseignements personnels* et de la *Loi sur l'accès à l'information*.

Pour les vérifications internes, le Commissaire donne au besoin des conseils d'ordre général et fait des commentaires ou des recommandations sur le degré d'observation, par le ministère ou l'organisme en cause, des règles sur la collecte, l'usage, la conservation, la divulgation et le retrait des renseignements personnels, en application de la Loi.

Emploi et Immigration est l'un des plus gros organismes fédéraux; il fournit des conseils et de la formation sur l'emploi à des millions de Canadiens qu'il aide à trouver du travail, en plus d'administrer le Régime d'assurance-chômage. En outre, il filtre les immigrants et leur fournit des services.

Les vérificateurs internes ont conclu que le besoin de protection de la vie privée était manifeste, étant donné qu'EIC, avec ses 800 bureaux, est une véritable mine de renseignements personnels. Sans renseignements personnels, EIC ne pourrait pas fonctionner. Le Commissaire n'aurait pas dit mieux.

Constatations

Connaissance de la Loi sur la protection des renseignements personnels: Les vérificateurs d'EIC ont constaté que les coordonnateurs de la protection de la vie privée connaissaient la Loi, mais que les autres employés n'étaient pas aussi bien informés. Par conséquent,

les demandes officieuses ou celles de tierces parties, comme les gouvernements provinciaux ou les groupes de pression, n'étaient pas toujours traitées de façon uniforme. EIC s'est donné pour priorité de produire des manuels d'exploitation à l'intention de l'ensemble de son personnel, qui bénéficiera aussi de cours de formation.

Collecte et usage des renseignements personnels : Les vérificateurs ont constaté que plusieurs formulaires servant à recueillir des renseignements personnels faisaient état de façon incomplète de la *Loi sur la protection des renseignements personnels*. Ils ont proposé à EIC d'améliorer son texte sur la protection de la vie privée en ajoutant des descriptions des données requises, de la façon de les utiliser, du fichier où elles sont conservées et des organisations avec lesquelles elles sont partagées. Ils ont aussi recommandé une amélioration de la description du fichier des dossiers de réclamation d'assurance-chômage qui figurent dans le *Répertoire de renseignements personnels*, parce que la description actuelle ne reflète peut-être pas très bien toutes les données conservées dans le fichier.

Pour s'assurer que ses formules respectent la *Loi sur la protection des renseignements personnels*, EIC demandera au personnel de ses programmes de consulter la Direction de l'application des droits du public au sujet des formules servant à recueillir des renseignements personnels.

Couplage des données : EIC partage ou couple sans doute plus de données avec d'autres organismes que n'importe quelle autre composante de l'Administration fédérale. Les couplages comprennent des comparaisons de données avec Revenu Canada (Impôt) pour vérifier si les particuliers déclarent leurs revenus et si les prestataires du régime d'assurance-chômage travaillent. Le couplage est effectué en vertu de la *Loi sur l'assurance-chômage* et de la *Loi sur l'immigration*.

La *Loi sur la protection des renseignements personnels* autorise aussi le couplage « aux termes d'accords ou d'ententes » entre des organismes gouvernementaux, d'autres gouvernements (soit provinciaux, soit d'autres pays) et des organismes internationaux, pour l'administration ou l'application d'une loi ou la tenue d'une enquête.

Les vérificateurs internes ont constaté que le couplage n'était pas toujours régi par des accords écrits et qu'une partie de ces accords datent de si longtemps qu'ils ne reflètent plus la législation actuelle. S'ils n'ont pas d'accords officiels pour se guider, les employés ne savent pas très bien quels renseignements peuvent être partagés et comment ils peuvent être utilisés. Les vérificateurs ont recommandé qu'on distribue des résumés des accords au personnel, que tous les accords en négociation soient conclus et qu'on procède ensuite à une vérification de suivi afin de s'assurer qu'EIC respecte bien la nouvelle politique du Conseil du Trésor sur le couplage des données.

EIC examinera tous les accords et conclura ceux qui ne l'ont pas encore été, en plus de signaler tous ses couplages de données actuels au Commissaire et de veiller à ce qu'ils soient tous mentionnés dans le *Répertoire de renseignements personnels*. (La nouvelle politique du Conseil du Trésor sur le couplage oblige tous les ministères et organismes à prévenir le Commissariat 60 jours avant tout nouveau couplage.)

Sécurité : Les vérificateurs d'EIC ont constaté que certains marchés de service avec des entreprises privées ne contenaient pas de dispositions sur la sécurité ou sur la protection des renseignements personnels, de sorte que ces entreprises risquaient de ne pas toujours traiter les renseignements de ce genre de façon confidentielle. Les vérificateurs ont donné des exemples d'entreprises ou de particuliers offrant des services de transport, de destruction de documents, de nettoyage de bureaux (particulièrement dans les bureaux à étagères ouvertes), d'interprétation, de transcription, de traitement électronique des données et de diagnostic psychologique.

Enfin, les vérificateurs ont recommandé que les marchés régionaux soient révisés par l'ajout de dispositions de protection des renseignements personnels conformément aux exigences de la *Loi sur la protection des renseignements personnels*, de la politique sur la sécurité et du règlement pertinent d'EIC.

Retrait des renseignements personnels : La vérification a révélé un manque d'uniformité des méthodes de destruction des documents personnels dans les bureau d'EIC. Dans certains cas, on trie les documents avant de les détruire en les envoyant à la déchiqueteuse ou en les mettant à la poubelle; ailleurs, on jette simplement les documents en même temps que les déchets des autres locataires de l'immeuble. Étant donné que le personnel des bureaux locaux estime que les documents contenant des renseignements personnels constituent jusqu'à 90 p. 100 des déchets, les vérificateurs se demandent s'il vaut la peine de les trier. En outre, ils ont constaté qu'aucun service ne tient de registre de contrôle et de destruction de ses microfiches. À cet égard, la procédure varie : on peut envoyer les vieilles fiches aux bureaux régionaux, à des centres régionaux d'informatique ou aux Archives nationales. Les vérificateurs ont proposé l'adoption d'une procédure normalisée de destruction des vieilles fiches.

Dans son plan de travail, le Groupe d'EIC sur la sécurité s'intéressera à la fois à l'ajout de dispositions sur la sécurité dans les marchés de services et au contrôle et à la destruction des microfiches dans son plan de travail.

Dossiers d'aide aux employés (PAE)

Ces dossiers sont parmi les plus délicats des dossiers personnels conservés par le gouvernement; ils contiennent des renseignements personnels sur des personnes recevant des service de counselling pour surmonter leurs problèmes de santé ou de comportement. Seuls l'employé intéressé et le conseiller peuvent consulter ces dossiers. S'ils étaient volés ou si leur contenu était divulgué sans autorisation, l'employé pourrait subir un préjudice irréparable.

Par conséquent, la vérification des dossiers du PAE pose des difficultés particulières, à la fois pour le ministère ou l'organisme en cause et pour le Commissaire. Celui-ci est déchiré entre la nécessité de veiller à ce que les renseignements soient consultés par le moins de personnes possible et son besoin de vérifier s'ils sont recueillis et protégés convenablement. Les vérificateurs examinent donc des dossiers anonymes, choisis au hasard, afin de déterminer si les renseignements qui y sont consignés répondent aux normes de collecte, d'usage, de conservation, de divulgation et de retrait nécessaires à la protection de la vie privée.

EIC n'avait pas de dossiers du PAE dans ses bureaux d'Ottawa, en raison de sa politique de conserver le moins de renseignements possibles en communiquant les détails nécessaires à des conseillers de l'extérieur. Cette décision de ne pas conserver de dossiers est compréhensible, voire louable, car c'est un bon moyen d'assurer la confidentialité aux bénéficiaires des services. Néanmoins, il s'ensuit que la direction ne conserve pas de trace des utilisations des renseignements ni de preuve du consentement des intéressés à leur divulgation.

Le Commissaire a constaté qu'EIC avait dû accepter un compromis en tenant compte à la fois de la nécessité de limiter la quantité de renseignements personnels délicats contenus dans les dossiers et le besoin de disposer des mesures de contrôle opérationnel voulues. Il a proposé au ministère de réétudier sa procédure actuelle.

Les vérificateurs ont fait plusieurs propositions en vue d'améliorations de la sécurité matérielle des dossiers du service et de la destruction des documents de rebut contenant des renseignements personnels. Le Commissaire a recommandé qu'EIC prenne les mêmes mesures d'amélioration dans ses bureaux régionaux qui conservent des dossiers.

Aviser le Commissaire

La *Loi sur la protection des renseignements personnels* interdit globalement aux organismes fédéraux de divulguer des renseignements personnels à quiconque sauf à l'individu concerné. Cette règle a des exceptions, comme presque toutes les règles. En fait, il y a 13 exceptions, allant des cas où les renseignements peuvent être exigés par mandat ou par subpœna, à ceux où leur divulgation peut aider les peuples autochtones à établir leurs droits ou à justifier leurs doléances.

Deux de ces exceptions obligent l'institution gouvernementale en cause à envoyer un préavis au Commissaire. La première porte sur la divulgation des renseignements « pour des raisons d'intérêt public » ou à l'avantage de l'individu concerné. La deuxième exception a trait aux divulgations « compatibles » avec les fins auxquelles les renseignements ont été recueillis, quand ces fins ne sont pas décrites dans le *Répertoire de renseignements personnels*.

La *Loi sur la protection des renseignements personnels* ne permet ni au Commissaire, ni à l'intéressé d'empêcher la divulgation. Par contre, la *Loi sur l'accès à l'information* donne à des tiers le droit d'en appeler aux tribunaux pour empêcher la divulgation de renseignements concernant des personnes morales. Le Commissaire à la protection de la vie privée estime que les particuliers devraient eux aussi pouvoir empêcher les divulgations qu'ils considèrent comme injustifiées et préjudiciables.

Au début, on craignait que ces exceptions à la règle générale interdisant la divulgation de renseignements personnels à des tiers percent une brèche monumentale dans la Loi. On redoutait une divulgation massive de renseignements personnels, fondée sur des interprétations laxistes de « l'intérêt public » et des usages « compatibles ». Pour prévenir les abus, le Commissaire a fait état de toutes les utilisations des divulgations dans son rapport annuel.

Jusqu'à présent, il ne semble pas y avoir d'abus manifestes. Même si le Commissariat continue d'étudier chaque préavis, le rapport annuel ne contiendra désormais que des statistiques globales et quelques exemples représentatifs. Cela dit, une ventilation détaillée des 24 préavis est disponible sur demande au Commissariat.

Les députés, une fois de plus

Une fois de plus, Emploi et Immigration Canada (EIC) a avisé le Commissaire de sa politique de réponse aux demandes de renseignements personnels sur leurs commettants que les députés lui adresseraient pendant la campagne électorale fédérale.

La *Loi sur la protection des renseignements personnels* autorise les organismes gouvernementaux à divulguer des renseignements personnels à un député qui cherche à aider un de ses commettants à résoudre un problème. Néanmoins, après la dissolution du Parlement, les députés sortants redeviennent des citoyens comme les autres. Autrement dit, si l'on s'en tient à la lettre de la Loi, ils ne pourraient

plus s'enquérir au nom de leurs commettants et sans leur permission expresse des démêlés de ceux-ci avec une institution gouvernementale, étant donné qu'ils devraient alors consulter des renseignements personnels.

Il semble doctrinaire de refuser d'autoriser les députés à aider leurs commettants pendant une campagne électorale où leur statut est en suspens. D'un autre côté, permettre à ces députés en campagne électorale d'avoir accès à des informations gouvernementales pourrait sembler les avantager au détriment des autres candidats leur faisant la course. Emploi et Immigration Canada, l'institution gouvernementale la plus souvent sollicitée, a informé le Commissaire de son intention de continuer à divulguer des renseignements personnels aux députés sortants pendant la campagne électorale, étant donné que « l'individu concerné en tirerait un avantage certain », conformément au sous-alinéa 8(2)m)(ii).

Le Commissaire a entériné cette pratique, la même que pour la campagne électorale de 1984. Toutefois, il a réitéré ses réserves, en disant que la délégation de la responsabilité de divulguer des renseignements personnels à « n'importe quel » agent ou employé d'EIC faisait augmenter les risques d'abus. Le personnel du Commissariat a donc examiné 1479 avis de ce genre pendant la compagne électorale.

La *Loi sur la protection des renseignements personnels* devrait être modifiée avant les prochaines élections, pour qu'il devienne désormais légalement possible pour les députés de continuer à avoir accès aux renseignements dont ils ont besoin pour pouvoir aider leurs commettants en période de campagne électorale.

La propriétaire d'un chien n'a pas respecté la période de quarantaine.

La Société canadienne des postes a avisé le Commissaire qu'elle avait donné à un vétérinaire d'Agriculture Canada la nouvelle adresse d'une femme qui semblait n'avoir pas respecté la période de quarantaine de six mois de son chien. La bête avait été en contact avec un animal enragé, et son traitement n'était pas terminé.

La Société des postes avait communiqué directement avec l'intéressée, mais celle-ci avait refusé de collaborer. Bien que la *Loi sur les maladies et la protection des animaux* n'autorise pas la divulgation de ces renseignements, la Société a conclu que leur communication s'imposait dans l'intérêt public. Le Commissaire n'a pas contesté la divulgation.

Les noms et adresses des détenus devaient être communiqués au Directeur général des élections

Après qu'un tribunal manitobain eut décidé que les détenus avaient le droit de voter aux élections fédérales, le Service correctionnel du Canada a avisé le Commissaire qu'il communiquerait au Directeur général des élections du Canada les noms et adresses de tous les détenus fédéraux incarcérés au Manitoba.

La liste des détenus devait permettre aux directeurs des élections d'organiser le scrutin dans les pénitenciers; elle ne devait être communiquée à personne d'autre. Toutefois, comme la cause a été portée en appel, les détenus n'ont pas été recensés et la liste n'a pas été envoyée.

Le gouvernement soviétique a été averti de la visite d'une personne atteinte d'une maladie

Le ministère des Affaires extérieures a avisé le Commissaire qu'il avait averti les services de santé de l'Union soviétique de la visite en URSS d'une Canadienne atteinte d'une maladie infectieuse.

Santé et Bien-être social Canada avait prévenu les Affaires extérieures qu'une femme souffrant de tuberculose pulmonaire avait refusé les médicaments qu'on voulait lui administrer et qu'elle avait décidé de quitter l'hôpital. Par la suite, elle était allée visiter des parents en Union soviétique. Après avoir communiqué avec le Commissariat, le ministère des Affaires extérieures a transmis les renseignements à l'ambassade du Canada à Moscou, laquelle a averti le gouvernement soviétique.

La divulgation a été considérée comme d'intérêt public.

Faites passer

On a prétendu naguère que s'il existait au Canada une confrérie de défenseurs de la vie privée, c'est-à-dire un groupe de militants avisés, elle tiendrait dans la salle de conférence du Commissaire à la protection de la vie privée. Pourtant, même le personnel du Commissaire y serait à l'étroit.

Aujourd'hui, les défenseurs de la vie privée ne sont plus aussi isolés. On l'a bien vu dans les deux conférences récentes sur la protection de la vie privée et l'accès à l'information où l'auditoire a rempli de grandes salles de réunion dans des hôtels de Toronto et d'Ottawa. Les défenseurs fédéraux et provinciaux et les promoteurs indépendants de la protection de la vie privée commencent à s'unir en un réseau non structuré qui s'allie avec des administrateurs éclairés de dossiers et de systèmes de TED pour prêcher la bonne parole.

Le public se pose peut-être encore des questions quand on lui parle de la *Loi sur la protection des renseignements personnels* (et il sourit à l'idée d'un Commissaire à la protection de la vie privée), mais il comprend la nature du problème et il en reconnaît toute la gravité.

Le Commissaire et ses collaborateurs saisissent toutes les occasions de parler de la Loi et des problèmes sous-jacents. Au cours de l'année, le Commissaire a prononcé une vingtaine de discours dans de nombreuses villes du pays devant divers groupes du Canadian Club, et il s'est adressé notamment à des agents de sécurité en formation, des spécialistes du traitement des données, des responsables d'organismes fédéraux et des cadres moyens spécialisés en gestion financière. Il a aussi participé à une séance d'information de la Chambre de commerce du Canada, au sujet des implications pour le secteur privé de la législation sur la protection des renseignements personnels et des lignes directrices de l'OCDE, et il a contribué à un séminaire sur le SIDA organisé par la Commission nationale des libérations conditionnelles.

Le Commissaire a entrepris une série de visites dans les pénitenciers fédéraux afin de parler de la *Loi sur la protection des renseignements personnels* avec le personnel et avec les détenus. Jusqu'à présent, il s'est rendu à la prison des femmes de Kingston et à l'établissement à sécurité moyenne de Springhill, en Nouvelle-Écosse.

Le personnel du Commissariat continue à donner des séances d'information aux participants aux cours de formation en gestion du gouvernement; il s'est en outre adressé à des employés de la Garde côtière, à Halifax, ainsi qu'aux participants à un séminaire sur les relations raciales, à Montréal, et à des étudiants du niveau collégial, à Toronto et à Ottawa.

Le Commissariat a produit un ensemble d'information intitulé « Avez-vous besoin d'aide concernant la *Loi sur la protection des renseignements personnels?* » L'ensemble comporte une affiche, un signet et une brochure explicative décrivant le rôle du Commissaire et la façon de se prévaloir des services de son Commissariat.

Gestion intégrée

La Gestion intégrée fournit au Commissaire à l'information et au Commissaire à la protection de la vie privée des services dans les domaines suivants : finances, personnel, administration, informatique et bibliothèque.

Finances

Pour l'année financière 1988–1989, les Commissariats disposaient d'un budget de 5 074 000 $ et de 69 années-personnes, soit une augmentation de 1 152 000 $ et de 11 années-personnes par rapport à 1987–1988. Les coûts en personnel de 3 837 201 $ et les frais de services professionnels et spéciaux de 702 567 $ ont totalisé plus de 88 p. 100 des dépenses. Les 603 137 $ restant ont couvert tous les autres frais.

Personnel

La substantielle augmentation du nombre d'années-personnes accordées au Commissaire à la protection de la vie privée a entraîné une activité intense dans le domaine du personnel. Les nouveaux postes ont été classifiés, et il y a eu 42 mesures de dotation, dont deux nominations de cadres supérieurs. En outre, le Conseil du Trésor a procédé à la vérification biannuelle de la classification de l'effectif des deux Commissariats, et les postes de PM et d'IS ont été réévalués en fonction des nouvelles normes de classification.

Finances
Voici l'état des dépenses des Commissariats pour la période du 1er avril 1988 au 31 mars 1989

	Information	Vie privée	Gestion intégrée	Total
Salaires	1,268,673	1,469,048	568,480	3,306,201
Contributions aux régimes d'avantages sociaux des employés	202,500	246,600	81,900	531,000
Transports et communications	29,363	66,204	118,094	213,661
Information	57,681	38,815	1,526	98,022
Services professionnels et spéciaux	506,936	144,959	50,672	702,567
Location	2,898	64	5,294	18,256
Achat de services de réparation et d'entretien	1,337	5,112	21,940	28,389
Services publics, fournitures et approvisionnements	9,957	14,738	37,264	61,959
Construction, acquisition de machines et d'équipement	43,232	85,986	48,464	177,682
Autres dépenses	1,630	1,569	1,969	5,168
Total des dépenses	**2,124,207**	**2,073,095**	**945,603**	**5,142,905**

Administration

Les Commissariats ont déménagé aux troisième et quatrième étages de la Tour B du complexe de Place de Ville. Des mesures de sécurité améliorées ont été mises en œuvre dans les nouveaux locaux et un manuel de sécurité a été rédigé. En outre, les Archives nationales ont effectué une vérification de la gestion des dossiers.

Informatique

Un examen des services informatiques a été entrepris avec l'aide de consultants de l'extérieur. Le Commissariat mettra en œuvre les principales recommandations de l'étude sur le renouvellement du système de gestion des affaires et l'expansion des systèmes de production de rapports et de textes.

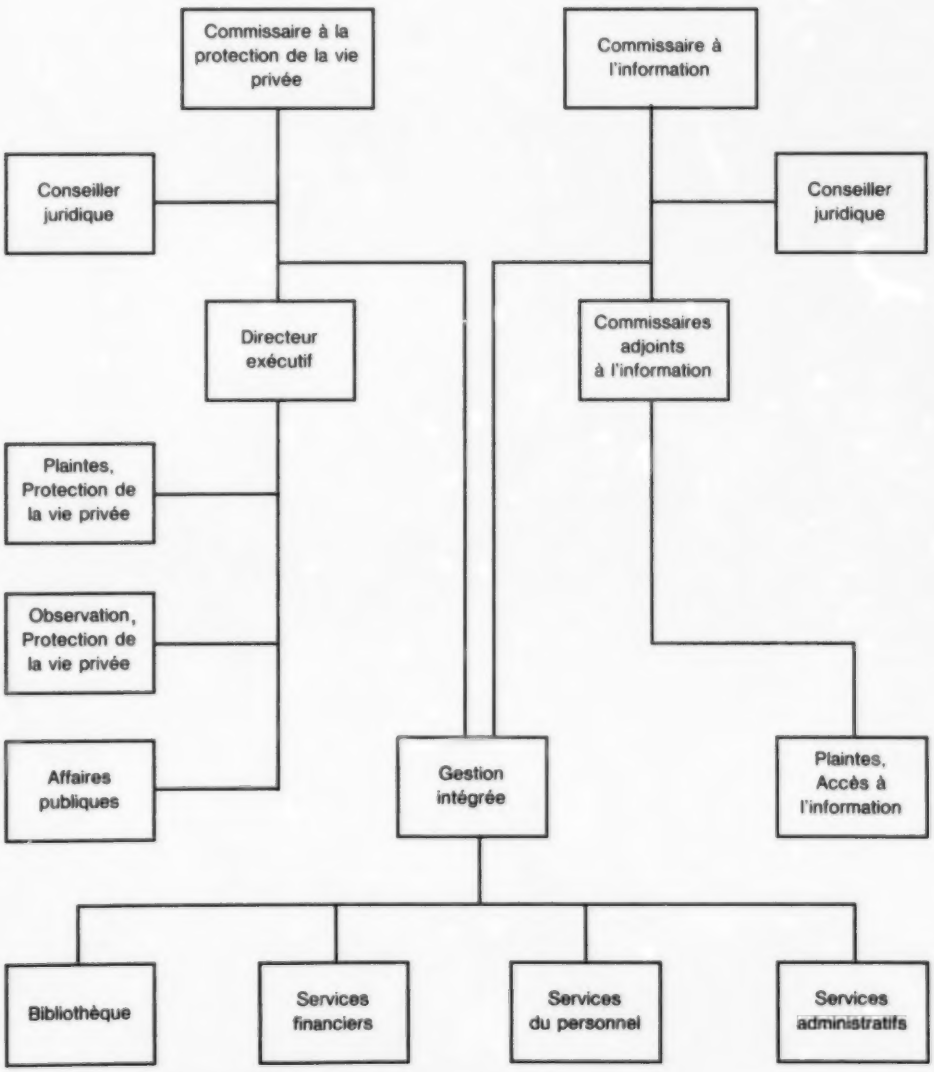
Bibliothèque

La bibliothèque continue d'offrir un service d'information et de référence aux deux Commissaires. Elle dispose de toute la gamme des services de bibliothèque, y compris les prêts interbibliothèques, les systèmes de référence automatisés et la recherche documentaire.

L'an dernier, environ 500 publications sur l'accès à l'information, la protection de la vie privée et le rôle de l'ombudsman ont été ajoutées à la collection. Le public est admis à la bibliothèque pour consulter les ouvrages, les dossiers de coupures de journaux, les publications en série et les rapports annuels.

Annexe I

Commissariats
à l'information et à la protection
de la vie privée du Canada



Annexe II

Institutions fédérales assujetties à la Loi

Administrateur de l'Office du transport du grain

Administration de la voie maritime du Saint-Laurent

Administration de l'assistance à l'agriculture des Prairies

Administration de pilotage de l'Atlantique

Administration de pilotage des Grands Lacs, Limitée

Administration de pilotage des Laurentides

Administration de pilotage du Pacifique

Administration du pipe-line du Nord

Administration du rétablissement agricole des Prairies

Affaires des anciens combattants Canada

Affaires extérieures Canada

Affaires indiennes et du Nord Canada

Agence canadienne de développement international

Agence de surveillance du secteur pétrolier

Agriculture Canada

Approvisionnements et Services Canada

Archives nationales du Canada

Banque du Canada

Banque fédérale de développement

Bibliothèque nationale

Bourse fédérale d'hypothèques

Bureau canadien de la sécurité aérienne

Bureau de l'enquêteur correctionnel

Bureau de l'inspecteur général du service canadien du renseignement de sécurité

Bureau du Conseil privé

Bureau du contrôleur général

Bureau de la coordonnatrice de la situation de la femme

Bureau du directeur des enquêtes et recherches

Bureau du Directeur général des élections

Bureau du directeur des enquêtes et recherches

Bureau du séquestre (biens ennemis)

Bureau de services juridiques des pensions

Bureau du Surintendant des institutions financières Canada

Bureau du vérificateur général

Centre canadien d'hygiène et de sécurité au travail

Centre de recherche pour le développement international

Centre national des Arts, Corporation du

Comité externe d'examen de la Gendarmerie royale du Canada

Comité de surveillance des activités de renseignement de sécurité

Commissariat aux langues officielles

Commission des allocations aux anciens combattants

Commission d'appel de l'immigration

Commission d'appel des pensions

Commission canadienne des droits de la personne

Commission canadienne d'examen des exportations des biens culturels

Commission canadienne des grains

Commission canadienne du blé

Commission canadienne du lait

Commission de la Capitale nationale

Commission canadienne des pensions

Commission canadienne des transports

Commission des champs de bataille nationaux

Commission de contrôle de l'énergie atomique

Commission de l'emploi et de l'immigration du Canada

Commission d'énergie du Nord canadien

Commission de la Fonction publique

Commission de l'immigration et du statut de refugié

Commission d'indemnisation des marins marchands

Commission des lieux et monuments historiques du Canada

Commission nationale des libérations conditionnelles

Commission des plaintes du public contre la Gendarmerie royale du Canada

Commission de réforme du droit du Canada

Commission des relations de travail dans la Fonction publique

Commission de révision de l'impôt

Commission de révision des lois

Commission du système métrique

Communications, Ministère des

Conseil des Arts du Canada

Conseil canadien des normes

Conseil canadien des relations de travail

Conseil consultatif des districts bilingues

Conseil consultatif de la situation de la femme

Conseil de contrôle des renseignements relatifs aux matières dangereuses

Conseil de développement de la région de l'Atlantique

Conseil économique du Canada

Conseil de fiducie du Fonds canadien de recherches de la Reine Élisabeth II sur les maladies de l'enfance

Conseil national de commercialisation des produits de ferme

Conseil national de l'esthétique industrielle

Conseil national de recherches du Canada

Conseil de la radiodiffusion et des télécommunications canadiennes

Conseil de recherches médicales

Conseil de recherches en sciences humaines

Conseil de recherches en sciences naturelles et en génie

Conseil de révision des pensions

Conseil des Sciences du Canada

Conseil des subventions au développement régional

Conseil du Trésor, Secrétariat du

Consommation et Corporations Canada

Construction de défense (1951) Limitée

Corporation commerciale canadienne

La Corporation du Pont international de la voie maritime, Ltée

Défense nationale

Directeur de l'établissement de soldats

Directeur des terres destinées aux anciens combattants

Emploi et Immigration Canada

Énergie, Mines et Ressources Canada

Environnement Canada

Finances, Ministère des

Gendarmerie royale du Canada

Industrie, Sciences et Technologie

Institut canadien pour la paix et la sécurité internationale

Investissement Canada

Justice Canada, Ministère de la

Monnaie royale canadienne

Musées nationaux du Canada

Office Canada-Nouvelle Ecosse des hydrocarbures extracôtiers

L'office Canada-Terre-Neuve des hydrocarbures extracôtiers

Office canadien du poisson salé

Office canadien des provendes

Office de commercialisation du poisson d'eau douce

Office des eaux des territoires du Nord-Ouest

Office des eaux du territoire du Yukon

Office des indemnisations pétrolières

Office national de l'énergie

Office national du film

Office des normes du gouvernement canadien

Office des prix des produits de la pêche

Office des produits agricoles

Office des recherches sur les pêcheries du Canada

Office de répartition des approvisionnements d'énergie

Office de stabilisation des prix agricoles

Pêches et Océans Canada

Les Ponts Jacques-Cartier et Champlain Incorporée

Revenu Canada

Santé et Bien-être social Canada

Secrétariat des relations fédérales-provinciales

Secrétariat d'État

Service canadien des pénitenciers

Service canadien du renseignement de sécurité

Service national des libérations conditionnelles

Société canadienne des brevets et d'exploitation Ltée

Société canadienne d'hypothèque et de logement

Société canadienne des ports

Société canadienne des postes

Société d'assurance-dépôt du Canada

Société de développement de l'industrie cinématographique canadienne

Société du crédit agricole

Société immobilière du Canada limitée

Société pour l'expansion des exportations

Solliciteur général Canada

Statistique Canada

Transports Canada

Travail Canada

Travaux publics Canada

Tribunal canadien du commerce extérieur